Liikenne- ja viestintävirasto

Explanatory memorandum
DRAFT

Record No TRAFICOM/36420/03.04.05.00/2025

Määräys viestintäverkon kriittisistä osista perustelumuistio

Table of contents

General rationale for the Regulation....2

1 Background to the regulation and its legal basis....2

2 Other relevant regulations of the Finnish Transport and Communications Agency....3

3 Objective of the regulation....4

4 Drafting of the regulation....5

5 Other implementation options....6

5.1 Regional and access networks and the use of priority classification as one of the criteria for criticality....6

5.2 Networks based on 5G technology....9

5.3 Theassessment of the criticalityof network management systems....13

5.4 Activities supporting services at the edge of the network....15

6 Feedback....17

7 Amendments....18

8 Assessment of the impact of the regulation....18

Detailed rationale....22

1 Scope....22

2 Definitions....22

2.1 Critical part of a communications network....22

2.2 Critical separate network and separate network operator....23

2.3 Separate network operator....24

2.4 Component of a communications network or service....24

2.5 4G network....25

2.6 5G network....25

2.7 Concepts defined in section 3 of the SVPL....25

3 Identification and documentation of critical parts of the communications network....26

3.1 Obligation toidentify and document the telecommunications company and separate networkoperator....26

3.2 Assessment of the criticality of 4G base stations in a separate network....27

4 Critical parts of a communications network....28
4.1 Definition of critical parts....28
4.2 Critical features of the communications network....28
5 Critical parts of the 4G network....40
5.1 Definition of the critical parts of a 4G network....40
5.2 Critical features of a 4G network....42
6 Critical parts of the 5G network....45
6.1 Features of a 5G network and its architecture....45
6.2 Definition ofcritical parts of the 5G network....46
6.3 Critical features of a 5G network....47
6.4 International comparison of critical parts of the 5G network....56
7 IP-based telephone services in a mobile network....56
8 Entry into force and transition period....57
Monitoring....58
References....59

General rationale for the Regulation

1 Background to the regulation and its legal basis

Section 244a of the Act on Electronic Communications Services (laki sähköisen viestinnän palveluista 917/2014; hereinafter referred to as “SVPL”; He 98/2020) governs equipment used in critical parts of a communication network. Subsection 1 states that a communications network device must not be used in critical parts of a public communications network if there are strong grounds for suspecting that the use of the device would endanger national security or national defence in such a way as to enable foreign intelligence or activities that would disrupt, paralyse or otherwise adversely affect Finland’s important interests, the basic functions of society or the democratic social order. According to said section, critical parts of a communications network include key functions and procedures to control or manage access to the network and traffic in the network in a significant manner.

Under section 244 a(6) of the SVPL, the Finnish Transport and Communications Agency (hereinafter also referred to as “Traficom”) lays down more detailed rules on the technical definition of communications networks, their critical parts in particular, taking into account recommendations of the Advisory Board for Network Security referred to in section 244 b. In the preparatory work on the regulation, account was taken of the recommendation of the Advisory Board on Network Security of 16 June 2025 regarding the regulation on the critical parts of communications networks.

In the application of section 244 a(1) of the SVPL, the assessment of the criticality of a part of a communications network may distinguish between determining whether there are strong grounds for suspecting that national secu-

rity or national defence will be compromised by the use of the communications network device. This regulation does not concern the assessment of the '*endangerment condition*' as, according to subsection 6, Traficom's mandate is limited to the technical definition of the critical parts of communications networks.

On 29 January 2020, the EU Member States published a common toolbox[1] to manage and resolve security risks. This regulation contributes to the implementation of a common toolbox for the security of the EU's 5G networks for the protection of critical parts of the network.

In addition to section 244 a(6) of the SVPL, the mandate of the Finnish Transport and Communications Agency is based on that subsections 1, 3 and 12 of section 244 of the Act. Under point 1 of that section, regulations issued by the Finnish Transport and Communications Agency may cover, for example, priority classification, and under point 3, information security and integrity and their maintenance, monitoring and network control, and under point 12, the format of related documents and data storage.

2 Other relevant regulations of the Finnish Transport and Communications Agency

Regulation M67 of the Finnish Transport and Communications Agency of 16 February 2024 on information security in telecommunications (TRAFICOM/248815/03.04.05.00/2022) defines minimum requirements for information security for telecommunications operators. The purpose of this regulation is to ensure that information security is a routine consideration in telecommunications companies. The regulation aims to ensure that information security matters are routinely considered through effective processes as part of the implementation of communications networks and services.

The Regulation of the Finnish Transport and Communications Agency on the verification of communications networks and services and on the synchronisation of communications networks of 17 June 2021 (TRAFICOM/54045/03.04.05.00/2020) imposes minimum obligations on telecommunications companies in such matters as securing the power supply of equipment used in the implementation of communications networks and services, the verification of equipment and connections, and the physical protection of equipment.

The Finnish Transport and Communications Agency's Regulation 66 A/2019 M of 2 December 2019 on disruptions to telecommunications operations deals with various kinds of disruption to telecommunications operations. The regulation covers, on the one hand, situations where a telecommunications company's service is subject to, or is threatened by, a significant breach of security (*an information security incident*) and, on the other, events which prevent or substantially interfere with the performance of the communication service (*a functionality failure*). The regulation imposes obligations on telecommunications companies regarding the detection and management of information security incidents and functionality failures, as well as on related reporting and statistics.

A recommendation on *contingency planning for telecommunications operations* (Recommendation 311) gives advice to telecommunications companies

[1] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

on compliance with the contingency requirements under the Act. The recommendation, which is partly confidential, is not a general, comprehensive guide on continuity or contingency planning and their implementation. Instead, it covers issues that the Agency recommends that telecommunications companies take into account as part of their contingency obligation and their existing contingency procedures.

Regulation 58 C/2023 of the Finnish Transport and Communications Agency of 22 November 2023 on the quality and universal service of communications networks and services (TRAFICOM/434071/03.04.05.00/2021) concerns the measurement and assurance of the reliability (including the operational reliability), performance and quality of communications networks and services. In this context, the regulation lays down general obligations applicable to all public communications networks and services, as well as specific requirements for telephone, internet access and television services.

The Regulation of the Finnish Transport and Communications Agency of 22 November 2024 on the technical implementation and verification of emergency transport services (TRAFICOM/628126/03.04.05.00/2023) contains requirements that, in the case of public communications networks, ensure the transfer of emergency calls and text messages as well as essential information related to them from communications networks to emergency centres. The requirements of the regulation also ensure that emergency calls are more likely to go through than normal calls in the event of a variety of backlog situations and disruptions in the communications network.

3 Objective of the regulation

The purpose of the regulation is to define the critical parts of a communications network. The regulation describes, under the rationale for the Government proposal (HE 98/2020) and the report of the Transport and Communications Committee (LiVM 16/2020), the critical technical parts of a network, i.e. the basic key functions and procedures to control or guide access to the network and traffic in the network.

The aim of the update to the regulation is to take account of the development of communication technologies, and in particular the development of 5G network technology in mobile networks, with consideration being given to its key societal role.

The regulation guides telecommunications companies and separate network operators covered by the regulation in the design of networks, the procurement of network equipment and the construction, maintenance and management of networks. This regulation promotes national security and information security in communications networks.

The regulation specifies the parts of the communications network that could be subject to the obligations and decisions under section 244a(1) and (2) of the Act on Electronic Communication Services. The regulation thus clarifies the scope of that section, even though the critical parts are not defined exhaustively.

4 Drafting of the regulation

According to the preliminary work for the Government proposal (HE 98/2020), the technical specifications of the regulation must take into account the international standards on the basis of which communications net-

works are designed and constructed. In particular, the drafting of the regulation relied on ETSI standards and technical 3GPP specifications, which were taken into account in the definition of the critical parts of 4G and 5G networks.

In October and November 2022, Traficom gave telecommunications companies and other key stakeholders an opportunity to present their views on the possible needs for amendments to the regulation and to answer related questions. Traficom received responses from DNA Oyj, Elisa Oyj, Telia Finland Oyj, Suomen Erillisverkot Oy and Huawei Technologies Oy (Finland) Co. Ltd and the Ministry of the Interior. At that time, on the basis of an overall assessment, the Agency considered that there was no urgent need to amend the regulation.

In January–February 2025, Traficom gave operators and key regulatory stakeholders covered by the regulation an opportunity to present their views on the possible need for amendments to the regulation and to answer related questions. Traficom requested a statement and received responses from DNA Oyj, Elisa Oyj, Telia Finland Oyj, Suomen Erillisverkot Oy, the Finnish Defence Forces, the National Police Board, FiCom ry, the Finnet Federation, the Ministry of Economic Affairs and Employment, the Ministry of Finance and the Ministry of the Interior. In addition, Oy Ericsson Ab gave a statement on its own initiative.

The regulation was drafted in broad collaboration with the industry, parties responsible for national security and national defence and other authorities. In January 2025, Traficom sent an invitation to all telecommunications companies and key authorities to participate in the drafting of the regulation.

In February 2025, one or more members of the working group were appointed from: the Finnish Transport and Communications Agency, the Prime Minister's Office, the Ministry of Finance, the Ministry of Defence, the Ministry of the Interior, the National Emergency Supply Agency, the Finnish Defence Forces, the Finnish Security and Intelligence Service, the National Police Board, Digita Oy, DNA Oyj, Elisa Oyj, Telia Finland Oyj, Suomen Erillisverkot Oy, FiCom ry and the Finnet Association. The following entities did not appoint anyone the working group: the Ministry of Transport and Communications, the Ministry of Economic Affairs and Employment, the Ministry of Justice, the Ministry for Foreign Affairs, the National Bureau of Investigation and the Finnish Border Guard. The working group met five times between February and May 2025. The members of the working group were given the opportunity to express their views on the individual amendments proposed by Traficom, as well as to comment more generally on the draft provisions and explanatory memorandum drawn up by the Agency.

From the early draft stage of the regulation onwards, the following parties participated in the preparation, either by commenting or by monitoring the work: [TBC]

There was an opportunity to comment on the draft text of the regulation and the explanatory memorandum in order to finalise the draft versions that would be circulated for xx.xx.2025 further comment.

When the regulation was being drafted, consideration was given to the recommendation of the Advisory Board for Network Security of 16 June 2025 on

the regulation on the critical parts of communications networks.[2] In its recommendation, the Advisory Board considered that in assessing the criticality of parts of a communications network it is necessary to take into account proactively the increase in the importance of communications networks for society as a whole, trends in the development of communications network technologies and changes in the operating environment. The assessment suggested that attention should be paid to EU policies and recommendations, as well as to general international developments. The Advisory Board's recommendation states that it is essential that the project and updated regulation on the regulation on the critical parts of a communications network should take into account these factors. The current regulation, published on 20 May 2021, does not include certain parts of the 5G network, such as the radio access network. According to the Advisory Board, the update work should include an assessment of the need to extend the regulation on the critical parts of the network to parts of the 5G network not covered by the current regulation, where applicable. This notion would gain support, according to the recommendation, from the general development in communications network technologies, the increasing importance of communications networks for the various functions of society, and the need to ensure national security in the most advanced communications networks.

According to the recommendation, the Advisory Board considers it important that the assessment of the criticality of communications networks takes into account the predictability and legal certainty of investments in communications networks and the international standards on which the construction of communications networks is based. It is therefore advisable to assess the need for possible transition periods in the update work, while considering the lifecycles and the objectives of the regulation.

5 Other implementation options

5.1 Regional and access networks and the use of priority classification as one of the criteria for criticality

During the preparatory work, the option of identifying 5G transmission connections as critical was considered. However, in the preparation, it was decided to consider instead a technology-neutral approach to extending the use of priority classification as one of the criteria for criticality. This would mean amending section 4.1 of the regulation so that components of a communications network or service in priority category 3 in accordance with the regulation on the verification of communications networks and services and on the synchronisation of communications networks, in addition to the previous priority categories 1 and 2, are also included as critical parts of the network.

Section 4 of the regulation specifies certain functions and procedures associated with a communications network on a technology neutral basis as critical parts of the network. When the regulation was being drafted, the Agency consulted certain parties on whether the application of the technology-neutral criteria under section 4 of the regulation on the definition of the critical parts of a network was in some respects open to interpretation. In the opinion of the respondents, the application of the definition of critical parts defined applying technology-neutral criteria in section 4 was not open to interpretation. During the preparatory work, the Agency consulted certain parties on the need for further clarification in the regulation regarding the assess-

[2] Recommendation of the Advisory Board on Network Security on the regulation of the critical parts of communications networks, 16 June 2025, VN/15573/2022.

ment of the criticality of the components of regional and access networks (e.g. in the case of a component serving a mobile network). The majority of respondents thought that there was no need to clarify the regulation in this respect, while others considered that it would indeed be necessary to clarify the provision in the case of regional or access networks serving critical parts of mobile networks. Some respondents did not express any opinion regarding the matter at all.

During the preparatory work, the Agency consulted certain parties on whether the use of priority classification as one of the criteria for criticality was a viable and proportionate option. The telecommunications companies that replied thought it a mainly viable option. On the other hand, some took the view that there were no essential challenges, but a purely volume-based definition for priority classification could lead to conflicts with the existing definitions in the law.

Following the consultations with stakeholders, the parties involved in the regulation project decided to consider the following options:

A) maintain the status quo;

B) components in priority categories other than 1 or 2 are also defined as critical;

C) components of a communications network or service are defined as critical when they route or transmit traffic between base stations of a 5G radio network and a 5G backbone network; or

D) components of a communications network or service that transmit or route traffic between the critical parts of the communications network and are in priority category 3 pursuant to the regulation on the verification of communications networks and services and on the synchronisation of communications networks are defined as critical.

Determining as critical the components of a communications network or service that route or transmit traffic between the 5G radio network and the 5G backbone network is supported by the fact that the essential services of new generation mobile networks, such as low latency and/or high capacity services (e.g. eMBB and URLLC services), rely essentially on functional and reliable transmission links between both base stations and the core network. In addition, mobile network management and monitoring traffic, as well as network synchronisation data, are transmitted via these transmission connections. The importance of time synchronisation via a fixed network is also stated in section 21 of the explanatory memorandum to the Regulation of the Finnish Transport and Communications Agency on the verification of communications networks and services and on the synchronisation of communications networks.

On the other hand, identifying and documenting components of a communications network or service that route or transmit traffic between critical parts of the network, such as the 5G radio network and the 5G backbone network, could prove challenging, in particular if transmission connections are acquired from a subcontractor. In certain situations, the definition option could also lead to a needless attempt to limit the range of traffic routing and transmitting equipment for the critical parts of the network, such as a 5G radio network, while potentially compromising the operational security of commu-

nications networks and services, in order to avoid the application of section 244 a of the SVPL. If the section were applied to the traffic-carrying component of any critical component rather than to the traffic-carrying and routing components of the 5G radio network alone, such partial optimisation would probably be significantly less likely. Any lack of clarity regarding the criticality of some components of communications networks or services would also be reflected in the regional and access networks serving that component.

The priority classification of the components of a communications network or service as laid down in the Finnish Transport and Communications Agency's regulation on the verification of communications networks and services and synchronisation of communications networks is based on the type of communications service, the number of users and the geographical area affected. - Compared to the specification that the connections between the base stations and the core of a 5G network are critical parts of that network, the option of *a definition based on the type of service and the user impact* would have the advantage of being a technology-neutral definition based on a prioritisation that complements the network technology-specific specifications and is seen as a workable and proportionate approach. The definition of technology-neutral critical parts will also fill gaps in the case of functions not separately described in the technical specifications referred to in the network technology-specific specifications. On the other hand, the option does not take good account of situations where the criticality of a component is based on ensuring the confidentiality of communications. In the case of a radio network, this challenge can be met by specifying the base stations of a 5G network as critical.

The current situation does not cover cases where the functionality may have been distributed across multiple devices, in which case the number of users of a single device may fall below the threshold based on the number of users. This would also support the classification of components other than components in priority category 1 or 2 as critical parts. However, the components in priority category 3 still affect a significant number of users. On the other hand, the priority category for a base station with basic coverage in the mobile network is always 5, and base stations other than those with basic coverage do not need to be prioritised. This would also support the inclusion of lower priority categories as critical parts of a network. However, the user-effect-based approach only complements the other criteria, so it cannot currently be considered appropriate to define the components in priority categories 4 to 5 as critical without exception.

In view of the above, the most reasonable option seemed to be also to define as critical parts of a communications network those components of a communications network or -service that fall under priority category 3 in the Regulation on the verification of communications networks and services and the synchronisation of communications networks, in so far as they transmit or route traffic between critical parts of a communications network or service.

Thus, a new subsection (iv) added to section 4(1) of the regulation defines as a critical part of a communications network the components of the communications network or service transmitting or routing traffic between critical parts of the communications network which fall under priority category 3 in the Regulation of the Finnish Transport and Communications Agency of 17 June 2021 on the verification of communications networks and services and the synchronisation of communications networks (TRAFICOM/

54045/03.04.05.00/2020). The new subsection iv is therefore only applicable to components of regional and access networks that serve the critical parts of communications networks as here described.

5.2 Networks based on 5G technology

The previous regulation on the critical parts of a communications network was adopted at a time when 5G networks were only just being rolled out in Finland. The technology development of 5G networks was partly incomplete and there was still no comprehensive information available on the more precise use and function of the technologies as part of the network. As a result, Traficom took the view that the potential criticality of certain components of the communications network or -service, such as the base stations of the 5G network, could not be addressed in the regulation until later. Insofar as the potential criticality of parts of the network was not addressed in the previous regulation, the case was left for individual assessment. directly pursuant to the definition of a critical part of the communications network as provided for by law.

In addition, it should be noted that in the case of 5G-NSA (Non-Standalone) networks, the radio network based on 5G technology relies on the core of the 4G network, i.e. the 4G technology also plays a critical role in 5G-NSA networks. It should also be noted that there are several interfaces between 4G and 5G networks in order to ensure interoperability (EPC-5GC interworking), and there may be interdependence between networks.

A key use case of the 5G NSA network is the growth in the transmission capacity of the radio network. The 5G NSA network is based on the EPC core (Evolved Packet Core) of the 4G network. The 5G-NSA networks will not yet undergo a paradigm change in network nature, and new use cases of the 5G network will not be widely implemented, despite the development versions. The 5G NSA network will be updated for functionality during its life cycle.

The 5G components of a 5G NSA network would be covered by the definition of the critical parts of a 5G network in terms of the scope of application. For example, if some parts of a 5G network were identified as critical, they would also be critical in the context of a 5G NSA network. Similarly, in the case of 5G NSA networks, -the criticality of the 4G network components used could be assessed basically according what would be set down for 4G network parts in the regulation. 5G base stations (gNodeB/en-gNodeB, gNB/en-gNB) are also used in 5G NSA networks based on the 4G network core, with the key use case of the 5G base stations being the growth in radio network data transmission capacity.

While the regulation was being drafted, the Agency consulted certain parties on the list of critical functionalities of the 5G network included in the regulation, as to where it was comprehensive and actually up to date. The views of telecommunications companies on the update of the list of critical features of a 5G network vary: some thought that the list of critical features of a 5G network was indeed up to date and comprehensive. Some were of the view that it should be supplemented with the new Rel-17 and Rel-18 functions for the 5G core. Others thought that 5G base stations, and in particular the entity implementing the CU functionality of the radio network, should be defined as a critical component of the network. Other respondents also said that the list needed to be made more explicit in terms of new functionalities and extended to cover the 5G radio network.

A strong argument for the need for assessment is the fact that in the recommendation of the Advisory Committee on Network Security concerning the regulation on the critical parts of communications networks, the Advisory Committee considers that the need to extend the regulation on the critical parts of the network to include parts of the 5G network that were not included in the regulation published on 20 May 2021 should be assessed as necessary in the updated regulation.[3]

One of the key differences between the 5G network and the older networks is the redesigned service gateway-based network core based on software components. Traffic between the core functions of the network takes place along a standardised gateway. The standardised gateway enables fixed integration of service providers into the core of the 5G network. This enables the network to adapt in such a way a\that it can be optimised for the services used by users. Adding new components to the gateway without changing it is possible, for example, programmatically, by updating the software or by introducing new features.

New features implemented using the 5G technology, which are critical to the safety of society and users, will change the very essence of the entire network. A system that was largely based on data transfer and physical network elements will be transformed into a mostly software-based cloud service that refines data, where adequate controls must be defined to ensure security. 5G technology will be increasingly used to realise time-critical services and other services for specific use cases. Unlike in the past, data processing based on edge computing, in particular, can be carried out in the network itself, which will make the network different from the previous networks. It is also likely that in the future, functionalities previously implemented at the core of the network will also be transferred to the edge of the network, as the needs for performance and delay reduction, for example, will increase. The role of 5G and its services in mobile networks is also highlighted by the fact that previous generations of networks have already been phased out and are being decommissioned, leading to an increasing shift of 5G networks to mobile devices.

Given all this, there seems to be a good argument for re-examining and updating the definition of the critical parts of 5G networks is justified. However, the work on the definition still needs to prepare for the ongoing development of technical specifications and technology and the fact that the fact that the practical implementation of the networks is still partly unspecified. A base station consists of a base station unit and an antenna unit used to receive and transmit terminal equipment data traffic. In 2G technology, traffic passes through a separate base station controller (BSC), whereas in 4G and 5G technologies the base station transmits the traffic of users directly from the network interface of the telecommunications company or the private isolated operator to the core of the network. In addition, it should be noted that, with the increasing automation of the network, the functioning of several 5G base stations in the same geographical area is comparable to the effectiveness of a 2G network base station controller.

In the newer network generations, some of the functionalities of the base station controller, such as the management of radio resources, have been transferred directly to the base station. At the same time, antenna technology has evolved significantly. In particular, the 5G technology uses Solid MIMO (Multi-

[3] Recommendation of the Advisory Board on Network Security regarding the Regulation on the critical parts of communications networks, 16 June 2025, VN/15573/2022.

ple Input Multiple Output, MIMO), which enables the simultaneous service of multiple users. Massive MIMO technology features beamforming and precoding, allowing the base station to direct the signal straight to each terminal. This improves the quality of the connection, increases capacity, reduces interference and makes spectrum use more efficient.

Traficom thought previously that the specific features of 5G SA network base stations (gNodeB); also ng-eNodeB[4]) could not be assessed until later, as the technical development of base stations was still under way. Then it was thought that the definition of the architecture and use cases of base stations was still at the development phase in all the important aspects. The technological development that has taken place since then makes it possible to move more and more functions that control network operation, such as decision-making, computing power and intelligence, to the base station. These factors should be taken into account in the assessment of the criticality of a base station, in particular. Similarly, the development and intended use of network slicing and edge computing have been clarified to warrant a review of the criticality of the components. In addition to base stations, the criticality of trusted Wi-Fi networks or Wireline Access enabled by a 5G network, which may supplement an access network based on 5G base stations, must be assessed in more detail. Related functions specified by 3GPP include Wireline Access Gateway Function (W-AGF), Trusted Non-3GPP Gateway Function (TNGF) and Trusted WLAN Interworking Function (TWIF).

The criticality of radio access network components (e.g. A base station) is already high as an individual component or on a small scale, but becomes very critical if the whole network or a significant part of it is composed of those components. In mobile communications networks, the encryption of the users' traffic is terminated at the base station, which means that the base station has access to unencrypted network traffic. Overall, the availability, confidentiality and integrity of the user's traffic is thus at risk. Security controls cannot completely combat potential malicious functionalities contained in a component, such as backdoors contained in the software. It is possible to introduce potential malicious functionality into the radio network in such a way that the attack is not seen clearly as headed in the direction of the core of the network. The malicious functionality can also be utilised for attacks against other parts of the network; for example, it is possible to target the core functions of the network via a base station.

New use cases and the increased importance of connectivity reliability in functional and time-critical applications make even a single 5G network base station critical as regards the availability and functionality of such a service. In particular, new functionalities and use cases, including machine learning, capacity and traffic forecasting and optimisation, are poorly suited to static user numbers and coverage-specific priority determination, which explicitly supports the classification of radio access network components as critical. Automated network management, optimisation and forecasting based on machine learning pose new risks to the radio network. These factors would support the definition of gNB as a critical part of the network.

This option would also be strongly supported by the Recommendation of the Advisory Board for Network Security of 16 June 2025 regarding the regulation

[4] ng-eNodeB is an eNodeB defined in Rel-15 that works together with gNodeB when the core network is 5GC (3GPP TS 37.340, s. 4.1.3.1 and 4.1.3.2, see 4.1.3.1 and 4.1.3.2). This enables the implementation of new features (e.g. QoS, network slicing) enabled by a 5G core with the LTE radio technology. See also 3GPP TS 36.300, see 24.1 and 3GPP TS 38.300 see 4.1 and 4.2.

on critical parts of communications networks, in which the it took the view that the update of the regulation to cover parts of the network that were not covered by the 2021 regulation gains support from the general development of communications network technologies, the increased importance of communications networks for different functions of society and the assurance of national security in the most advanced communications networks. [5] In making the regulation clearer in terms of its content, account has also been taken of the international standards on which the construction of communications networks is based.

The update of the regulation as regards the 5G radio network also gains support from the recommendation of the Advisory Board that the assessment should give attention to EU policies and recommendations and to general international developments.[6] The Recommendation refers to the Commission's 2023 Communication on the safety of 5G networks, according to which Member States' measures to protect critical parts of 5G networks should also be extended to the Radio Access Network (RAN).[7] In the Communication, the Commission urges the Member States, when implementing these measures, also to focus attention as closely as possible on the recommendations presented in the progress report, in particular with regard to the scope of the restrictions, which should cover the critical and highly sensitive points identified in the EU coordinated risk assessment[8] , including the radio access network and the use of transition periods.

As regards the general international developments highlighted by the Advisory Board in its recommendation, it should be noted that, as the Advisory Board states in its recommendation, the radio access network has been identified as critical in a number of Member States, including Sweden, Lithuania, Portugal, Spain and Croatia. On the other hand, some Member States do not have reliable public data on the identification of radio access networks as critical. Member States have different approaches to defining critical parts of the network.[9] In France, the 5G radio access network is also covered by the measures[10].

In addition, as 5G technology continues to evolve, not only consumer users but also other user groups, such as machine-to-machine communications and industry-specific solutions (verticals) connected to the 5G network, need to be taken into account. The 5G network offers new services and applications that can be tailored to the needs of different users. The architecture of 5G networks features Network Function Virtualization (NFV), which allows the network to scale and adapt to different services and functions. These include, for example, a virtual backbone network, a cloud/centralised radio network,

[5] Recommendation of the Advisory Board for Network Security on the regulation of the critical parts of communications networks, 16 June 2025, VN/15573/2022.
[6] Recommendation of the Advisory Board for Network Security regarding the Regulation on the critical parts of communications networks, 16 June 2025, VN/15573/2022.
[7] Communication from the Commission – Implementation of the 5G Cybersecurity Toolbox, 15.6.2023, C (2023) 4049 final, p. 3.
[8] NIS Cooperation Group, EU coordinated risk assessment of the cybersecurity of 5G networks. Report. 9 October 2019. https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
[9] Recommendation of the Advisory Board for Network Security on the Regulation on the critical parts of communications networks, 16 June 2025, VN/15573/2022.
[10] Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et des communications électroniques. JORF n°0284 du 7 décembre 2019. The regulation covers the 5G radio network: New Radio Base Station (en-gNodeB and gNodeB).

C-RAN, edge computing and network slicing (5G Slice). In addition, automated network management, optimisation and forecasting assisted by AI/ML (Artificial Intelligence/Machine Learning, AI/ML) pose new risks to the radio network.

However, maintaining the status quo gains support from the fact that these functionalities may not be implemented in all cases. However, the predictability of the application of the regulation would support the classification of gNB as a critical part of the network, despite this.

Overall, the most reasonable option would appear to be to specify the provision by defining gNB, TNGF, TWIF, W-AGF, SMSF, DCCF, ADRF, NSACF and TSCTSF as critical parts of the communications network in 5G networks.

5.3 The assessment of the criticality of network management systems

Network management systems control and monitor network operations in real time and without them it would be a slow process or even impossible to respond to network failures. Network management systems can also be used to optimise traffic, load and possibly also the use of network resources in overload situations. The essential function of the systems is also to detect anomalies in traffic and to trigger reactions to such events, either automatically or by the staff of the telecommunications company. In 5G, more and more components operate on a cloud-based basis, which also highlights the importance of (information) security management in a distributed network.

During the preparatory work, the Agency consulted certain parties on the need to clarify the assessment of the criticality of the network management systems, for example by assessing the network management systems by network technology or by site of management.

Some respondents thought the current situation was appropriate. A few responses, on the other hand, suggested that some clarification was necessary. According to one respondent, the criticality of network control systems should be assessed on the basis of their central role in the network. A network management system is a highly critical resource and unverified access to a centralised management system compromises the security of the entire telecommunications network.

Matters assessed during the preparation process included, in particular, the criticality of the base station management system and how to define it appropriately in the regulation. In particular, the explicit definition of a 5G base station control system was examined as critical, but this proved to be unnecessary when 5G base stations (gNB) themselves were identified as critical.

Matters assessed during the preparation process included, in particular, the criticality of the base station control system and the appropriate manner of defining it in the regulation. The different options assessed were:

A) maintaining the status quo;

B) the definition of the management system for base stations in a 5G network and for the components that route or transmit traffic in the backbone network as critical; and

C) the identification of network management and network surveillance systems for components routing or transmitting traffic in critical parts of the communications network as critical.

Maintaining the status quo (option A) was not considered appropriate, as the management systems for the traffic-carrying and routing components of the critical parts of the network have the potential to affect or even entirely prevent users' access to the network and to interfere with the traffic transmitted by the component, for example by slowing it down.

The possibility of defining management systems for 5G base stations and components routing or transmitting backbone traffic as critical (option B) was assessed in the preparatory work. On the other hand, the definition of the components of the communications network or service that route or transmit traffic in a 5G radio network or a 5G backbone network might prove to be an arduous, challenging task. The definition option could also lead to a needless attempt to restrict the scope of equipment used to route and transmit 5G network traffic in order to avoid the application of section 244 a of the SVPL, while at the same time compromising the operational safety of communication services. Option B was not chosen because it was not considered appropriate to identify the transmission connection management systems of all 5G base stations as critical because the transmission connections can also be partially managed by other means, such as directly configuring individual equipment, in which case fault tolerance and crisis resistance can also be ensured in this way. The main transmission connections are often also duplicated, which means that the networks are able to operate, at least in part, even in emergencies automatically.

The preparatory work led to the definition of network management and control systems for components routing or transmitting traffic in critical parts of the communications network as critical parts of the network (option C). The advantage of this option is technological neutrality, which makes it last longer. In addition, the option does not have the negative impact associated with the other options mentioned above. A technology-neutral approach is also justified by the fact that the risk of the management systems for the traffic-transmitting and routing components of critical parts of the network having the potential to affect or even entirely prevent users' access to the network and to interfere with the traffic transmitted by the component does not apply just to the 5G network.

5.4 Activities supporting services at the edge of the network

In the preparation of the regulation, the Agency examined the need for an exception to the assessment of the criticality of network control functions at the edge of a network as provided for in section 7 of the regulation of 2021. This is especially relevant to edge computing. During the preparatory work, the Agency consulted certain parties on the application and necessity of the derogation.

The following options were examined in the preparation of the regulation:

A) maintaining the status quo; keeping the current exception according to which functions supporting services provided at the edge of a network are not critical parts of a communications network under certain conditions; and

B) annulment of the derogation: UPF (User Plane Function) and other core functions of the mobile network are always defined as critical parts of the network, even when they provide services at the edge of the network.

Maintaining the status quo, i.e. keeping the current derogation according to which the functions supporting services produced at the edge of the network are not critical parts of the communications network under certain conditions, necessarily entails a high threshold for the application of the derogation. Such a high threshold is due to the fact that the criteria must be able to ensure that a function does not meet the definition of critical part of the communications network. Despite this, it is not possible to define concrete ways of implementing protection mechanisms in advance; instead, the telecommunications company would be responsible for this. The necessary protection mechanisms will also depend on how these functions are used and how technology develops, such as how the interfaces of operations with other core network functions will be organised in the future[11]. The assessment of the adequacy of protection mechanisms is also a matter that, instead of referring to the regulation, it is more appropriate to carry out when assessing the condition governing damage under the Act. Additionally, with regard to a broad definition of the derogation/exception, it would be problematic if, with the development of networks, a significant number of network functions were not considered to be critical parts of a communications network in the longer term due to the exception to the regulation.

The cancellation of the exemption for edge computing would have the advantage of increased clarity and unambiguous application of the regulation. However, it is conceivable that the definition of these functions as a critical part of the communications network would, to some extent, influence their deployment and the decisions telecommunications companies make on the equipment manufacturers they use. The number of potential suppliers for a UPF function realised at the edge of a network is high, however, as they are not limited to the most well-known equipment manufacturers. This solution would be preferable to the uncertainty regarding how important control at the edge of the network will eventually be in 5G networks and for which purposes edge computing will be used in practice. It is conceivable that the transition of network functions to the edge may become more common when fast response time and optimisation of available capacity is essential. In such a case, this definition option would ensure that these functions are not excluded from the application of section 244 a of the SVPL.

Edge computing can be used to produce data processing services at the edge of a 5G network in cases where, for example, a very low delay is required. Edge computing enables the implementation of several service packages on the same platform. The service package may consist of one or more workloads produced on the platform, virtualised.[12]

The interfaces between edge computing and the core of the network can be seen to be particularly vulnerable to attacks and may have a major impact on the performance of the entire network. The main risk with edge computing is the exploitation of the platform in the event of an intrusion into another network or other workloads, or a denial-of-service attack elsewhere in the net-

[11] For example, it is possible that future versions of 5G network technical specifications will allow the opening of a gateway to user traffic and thus to UPF instead of being indirectly connected to the core via the Session Management Function (SMF), which controls user sessions.
[12] Components related to edge computing are described in, for instance, the ENISA Threat Landscape for 5G Networks, s. 3.9. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

work. The key means in which these risks may be realised include a programmatic intrusion through another workload, web or radio interface, or physical access to the equipment.

For edge computing, the core functions of the network can be taken to the edge of the network or brought closer to the users of the network in another manner. In edge computing, network core functions, such as a 5G network UPF (User Plane Function) or a local copy thereof, or other core functions defined by default as critical parts of a network in section 6 of the regulation, can be implemented at the edge of the network. If user traffic is to be controlled and decompressed at the edge of the network, UPF must be implemented there. This requires interfaces with the actual core of the network. For this reason, UPF in particular is assessed in what follows and the reasons why UPF is, by default, a critical part of a communications network, at the edge of the network too, are highlighted.

The central role of UPF in the management and monitoring of user traffic at the edge of the network makes it by default a critical function in a 5G network, at the edge of the network too. UPF also implements other critical services, such as controlling, filtering, monitoring or re-routing of users' traffic to a local data network or the web via an N6 interface where necessary. UPF provides services and directs traffic to mobile network users from the radio access network (RAN) and non-3GPP networks. UPF also plays a key role in the interception of user traffic and the collection of invoicing data. UPF can be a function that is commonly used for all data traffic, session-specific or sliced. It can also be carried out on the edge computing platform, to which the user's traffic is directed through the N6 interface.

On the one hand, UPF decides on user traffic control, monitoring and, if necessary, the termination of traffic with respect to a local network or data network, in which case it is important to ensure the safety of the UPF itself. Key UPF security functions for user traffic include DPI (Deep Packet Inspection), encryption functions, and enabling interception of telecommunications for traffic on the edge of the network.

On the other hand, UPF also interacts with the Session Management Function (SMF), which controls the network's core user sessions and is directly connected to the SBA gateway, the security of which is critical for the network as a whole. UPF also interacts with the other functions of the network, and their use cases may vary, depending on the session, slice or application, for example. UPF requires a connection to the network's joint SMF so that user traffic can be transferred from one UPF to another if the user moves between several functions realised at different geographical locations, for example. The question is, therefore, whether the actual core of the network can be protected from the local implementation of the core functions of the network.

Given the potentially high importance of UPF as part of a network, a high threshold must be set in the regulation to considering it non-critical, even at the edge of a network. Factors that may have an impact on the assessment include, at least, the function only serving specific users and not providing access to a public communications network, such as the internet. The assessment may also be influenced by how resource requests for local activities are handled and monitored, and whether the local function is treated as a non-trusted one from the point of view of the security of the core network.

The application of the derogation and the impact of technological developments and the practical implementation of edge computing were examined in the ex-post monitoring of the regulation. It was then seen as justified to look again at whether there were still grounds for the derogation and assess in more detail the potential criticality of functions related to edge computing. The option to cancel the derogation (option B) can now be considered more justified overall.

The security threats related to edge computing and protection against them do not differ significantly from other similar infrastructure. Currently, the threshold for the application of the derogation has been quite high and has not been applied to any significant extent. Edge computing introduced into the local operator's facilities and environment can play a key role in the implementation of the content of special services and computing functions,[13] which itself would advocate the cancellation of the derogation.

6 Feedback

To be added later.

7 Amendments

Section 4.1 of the regulation on general technology-neutral critical parts of a communications network is amended so that components of a communications network or service that are in priority category 3 in accordance with the regulation on the verification of communications networks and services and on the synchronisation of communications networks, in addition to the previous priority categories 1 and 2, are also included as critical parts of the network when components in priority category 3 route or transmit traffic between the critical parts of communications networks. In addition, section 4.9 of the regulation was subdivided and network management and network surveillance systems for components routing or transmitting traffic on critical parts of the communications network was added to that section.

In addition, in the first subsection of section 6 of the Regulation on critical parts of a 5G network, a reference to the network functionality under section 4.1 of the 3GPP Technical Specification TS 38.300 was added and the reference to the core of the 5G network was deleted. A reference to technical specification TS 38.300 of the 3GPP was also added to the second subsection of section 6. The changes necessitated by the added references were made to the section. The items gNB, TNGF, TWIF, W-AGF, SMSF, DCCF, ADRF, NSACF and TSCTSF were added to Table 2 of section 6 of the regulation.

The exemption from the regulation to the definition of a critical part for functions supporting services provided at the edge of a network in section 7 of the previous regulation was cancelled. The former section 8 of the regulation is now section 7. At the same time, the second subsection of section 3 of the Regulation on the identification and documentation of critical parts of a communications network was deleted following the cancellation of section 7 of the regulation.

8 Assessment of the impact of the regulation

The regulation is essentially based on an earlier regulation. The regulation project updates the Regulation on critical parts of a communications network that entered into force on 20 May 2021 (TRAFICOM/

[13] Finnish Transport and Communications Agency: Report on 5G cybersecurity. 28, p 8.

161584/03.04.05.00/2020). This regulation clarifies the definition of the critical parts of communications networks, taking into account the impact of developments in communication technologies, in particular the development of 5G network technologies in mobile communications networks, as well as their key role in society.

The regulation will now guide telecommunications companies and the separate network operators it covers in the design of networks, the procurement of network equipment and the construction, maintenance and management of networks. This regulation update will promote national security and information security in communications networks. The clarifications to the regulation will significantly lessen the uncertainty over the choices of equipment for operators by specifying the parts of the communications network which may be subject to the obligations under section 244 a(1) and (2) of the SVPL and its decisions under subsection 3. In this respect, the change will help protect the property of the operators, as they will be able to consider the more specific regulation when they acquire equipment in the future.

These impacts are consistent with the Advisory Board on Network Security's recommendation of 16 June 2025 on the Regulation on the critical parts of communications networks, according to which it though it important that the assessment of the criticality of communications networks takes into account the predictability and legal certainty of investments in communications networks and the international standards on which the construction of communications networks is based. It is therefore advisable to assess the need for possible transition periods in the update work, all the while considering the lifecycles and the objectives of the regulation.

The amendments to the regulation are not expected to have a decisive impact on the workload of the authorities.

No changes are proposed to the obligation to identify and document critical parts of the communications network itself in section 3 of the regulation, but changes to other sections can be expected to cause network operators to incur not more than minimal costs when defining and documenting critical parts of their networks and the components used therein, at least where the assessment is not conducted with reference to a previous regulation. The transition period for the application of the regulation is expected to reduce the costs involved substantially.

The amendment to section 4.1 of the Regulation on defining the common critical parts of different networks so that components of a communications network or service in priority category 3 under the Regulation on the verification of communications networks and services and synchronisation of communications networks, in addition to the previous priority categories 1 and 2, are also included as critical parts of the network, will widen the scope of the regulation. The new subsection iv would mean that components in priority category 3 would only be critical parts of a network when routing or transmitting traffic between the critical parts of communications networks.

At the same time, the unnecessary reference to the number of users or the area affected of/by the component is deleted. In practice, the deletion of the reference to the number of users or the area affected of/by the component applies only to base station controllers of previous generations of mobile networks, the priority category of which is always at least 2, regardless of the number of users or the area affected, according to the Regulation on the veri-

fication of communications networks and services and the synchronisation of communications networks. If base station controllers are thought to be critical parts of a communications network, it may be that this will have the same impact as reckoning hereinafter the base station control system to be a critical part of the communications network, if it is not financially and functionally possible to operate the base stations without base station controllers from the same manufacturer.

The definition of network management and network control systems for components routing or transmitting traffic in critical parts of a communications network as a critical part of the network may also indirectly affect choices of supplier made by a telecommunications company or a separate network operator, and that extends to system-managed network components. Even if a certain network management and network control system for components routing or transmitting traffic in the critical parts of the communications network were considered to be a critical part of the communications network, the telecommunications company could nevertheless opt for communications network equipment, the use of which may potentially pose a higher risk of realising the obligations under section 244(1) or (2) of the SVPL or a decision under subsection 3. Even in the case of a critical part of a network, the operator could endeavour to show that the use of that management system in the network does not compromise national security or national defence in any case. It could try to show this by, for example, introducing additional controls to guarantee information security. In this case, different security level segments may emerge in the management environment, and ensuring their separation and security is crucial. As section 244 a of the SVPL is based on ex post controls, it would not be possible for the operator to eliminate in advance the risk that the control system in question might have to be removed in the future. In addition, however, it is worth noting that, depending on the specific nature of the case, the network management and network control system for the components routing or transmitting traffic would not necessarily be a critical part of the communications network on the basis of the regulation if the controlling component did not route or transmit traffic in the critical parts of the network.

On the other hand, even if controlling network equipment were not considered critical parts of the communications network, the telecommunications company, having assessed the risks, could conclude that it would not be sensible to acquire the equipment without the same supplier’s control system if the control system were considered a critical part of the communications network. Such a solution could result if an economically and functionally sound system for controlling base station elements, independent of supplier, was not available or its development was not possible, and if the telecommunications company thought the risk too great that the control system might have to be removed during the lifecycle of the controlling network equipment without full compensation. The end result of the assessment could be that the operator's potential range of equipment suppliers could be restricted. This could have an impact on the negotiating position of the operator and on the competitive situation between equipment suppliers. However, such an impact is thought to be limited.

Clarification of the section on critical parts of the 5Gnetwork by adding a reference to the 3GPP Technical Specification TS 38.300 in section 6 of the regulation would clarify the regulation and the predictability of its application with regard to the functionalities and functions defined in that Technical Specification. The amendment can be expected to reduce the burden of com-

pliance with section 244 a of the SVPL and this regulation for telecommunications companies and separate network operators. Similarly, the addition of items gNB, TNGF, TWIF, W-AGF, SMSF, DCCF, ADRF, NSACF and TSCTSF in Table 2 of section 6 of the regulation dispenses with the uncertainty relating to the need for the telecommunications companies and separate network operators themselves to assess their criticality with reference to the state of the art and, for example, the functions and procedures performed by the component.

The regulation would cancel the exemption on the basis of which a feature linked to the control of a network supporting services produced at the edge of a 4G or 5G network, which in itself is one of the core functions of the communications network, could exceptionally be considered other than a critical part of the communications network. The cancellation of the exemption for functions supporting services provided at the edge of the network will boost the regulation’s legal certainty by making it more consistent and clearer. The purpose of the cancelled exemption was so that the regulation would not needlessly apply to functions where it can be confirmed that the function in question must not be seen as one that controls access to the network or network traffic. However, the security threats and protection against them related to the components covered by the exemption do not differ significantly from the rest of the similar infrastructure. Currently, the threshold for the application of the derogation has been quite high and it has not been applied to any significant extent. The amendment may well improve the information security of public communications networks and promote national security.

Detailed rationale

1 Scope

According to section 1 of the regulation, the regulation applies to public telecommunications operations and to a separate network connected to the public communications network of key operators as regards the vital functions of society, as referred to in section 244 a(2) of the Act on Electronic Communications Services (917/2014).

The scope of the regulation covers all operators to which section 244 a of the SVPL applies, i.e. both telecommunications companies and separate network operators.

The regulation is not exhaustive. In addition to the parts of a communications network defined as critical in the regulation, section 244 a of the SVPL applies, which means that the critical parts of a communications network may also be determined directly according to the definition of the critical parts of a communications network in accordance with section 1 f the SVPL.

2 Definitions

This section defines the main concepts used in the regulation.

2.1 Critical part of a communications network

The definition of the critical part of a communications network corresponds to the definition in section 244 a (1) of the SVPL. According to said section, critical parts of a communications network include key functions and procedures to control or manage basic access to the network and traffic on the network. It follows from the definition that, in principle, each communications network has parts that are critical for the operation of that network.

It should be noted that a question separate from the assessment of the criticality of a part of a communications network is whether the use of a specific communications network device in a critical part of a network meets the 'endangerment condition' in accordance with section 244 a(1) of the SVPL. It is met if it states that there are strong grounds for suspecting that the use of the device would endanger national security or national defence in such a way as to enable foreign intelligence or activities that would disrupt, paralyse or otherwise adversely affect Finland's key interests, the basic functions of society or the democratic social order. This regulation does not concern the assessment of the endangerment condition as, according to section 6, Traficom's mandate is limited to the technical definition of the critical parts of communications networks.

In the Government proposal, the concept of a critical part of a communications network is further specified as follows (HE 98/2020, p. 261):

A critical part of a communications network would be considered to be the core of the network, in particular the functions and procedures used to control and manage the network and traffic within the network. In the case of the current network technology, the critical core consists of, for instance, that part of the backbone network that manages access for different users and maintains the status of the user connections. The critical part(s) of a communications network ensure the availability of services and the confidentiality of communications. The critical parts of a communications network also include those parts of the network that

ensure the security of the entire communications network. In the case of the existing networks, these functions and procedures have been implemented in the backbone network.

It is also possible to distinguish the critical parts of a 5G network, although the structure of a 5G network is more complex than that of the previous network generations. In future network generations, such as 5G and 6G networks, the critical parts should be defined in line with the current level of technological development. In the definition of the critical parts of a communications network, it would also be essential to assess who has real potential to influence the operation and characteristics of the part of the communications network or the operation and features of the communications network device therein.

In a report by the Transport and Communications Committee (LiVM 16/2020, p. 16), the definition of a critical part of a communications network is further specified in the manner required in a statement by the Constitutional Law Committee (PeVL 35/2020). According to the report, critical parts of a communications network only include key and basic functions and procedures to control or manage access to the network and traffic in the network. According to the report received by the Committee, the clarification was drafted in discussions between the various ministries. However, the Committee added the word ‘key’ to the amendment following the statement by the Constitutional Law Committee. It goes on to say that critical parts of a communications network play a key role in the performance, maintenance, confidentiality of communications and security of the network.

It should therefore be noted that, when assessing the significance of the opinions on the critical parts of a communications network in the Government proposal, the scope of the critical parts was, in accordance with the Committee report, further specified to cover, rather than of network control and management, the control and management of *access to the network*. However, the concept of network access is not limited to the access of users to the network as specified in the Government proposal: the critical parts of a communications network can also control or manage other access to network functions and equipment, which may be based, for example, on network interconnections or control connections related to network maintenance. In addition, the concept of controlling or managing access to a network may include, for example, activities linked to ensuring the confidentiality of communications and the availability of network services, provided that they are also connected to the control of access to the network or its traffic.

On the basis of the report by the Transport and Communications Committee, it can be concluded that the priority and relevance increase if the function has an impact on the performance of the network, the maintenance of the network, the confidentiality of communications or the security of the network. In addition, it should be noted that functions related to the control or management of traffic in the network have been defined as critical parts of the communications network, as in the Government proposal, except that the concept of management has been replaced with the concept of control.

2.2 Critical separate network and separate network operator

Section 244 a (2) of the SVPL extends the scope of application of the section to separate networks connected to the public communications network of an operator that is essential for the function of a nuclear power plant, port, or airport or similar vital functions in society. These networks are referred to in the regulation as ‘critical separate networks’.

Section 244 a of the SVPL and the regulation will only apply to a separate network connected to a *public communications network*. The scope therefore covers only an 'inauthentic network' as a distinction from an actual separate network that is not interconnected in any way with a public communications network and is therefore not included in the scope of application of section 244 a of the SVPL.[14] Section 244 a of the SVPL does not apply to communications networks that are neither public communications networks nor critical separate networks, such as conventional networks for individual properties or companies. However, where the communications network is used to provide communications services to an unlimited circle of users, i.e. in the case of public telecommunications, section 244 a(1) of the SVPL and the points in the regulation on telecommunications companies apply[15].

Interconnection refers to, for example, a separate network implemented using the mobile communications network technology being connected to the internet by means of fixed network connection or the possibility of making calls outside the separate network. The applicability of section 244 a(2) of the SVPL does not therefore depend on, for instance, the interconnection of mobile networks or the potential for roaming.

A critical separate network may be a non-public communications network realised using any technology. According to the rationale for section 244 a of the SVPL, it is essential for the scope of application of subsection 2 that the communications network in question operates in such a critical environment from the point of view of society that if the core functions of the network were compromise, it could lead to a risk to national security or national defence (HE 98/2020, p. 262).

2.3 Separate network operator

The term 'separate network operator' refers to the owner or operator of a critical separate network as defined in section 2(2) of the regulation.[16] If, for example, a micro-operator provides as a service a critical separate network to an operator central to the vital functions of society, the micro-operator itself is also considered a key operator in terms of the functions vital to society. The obligations of the regulation thus cover the owner or other operator of a critical separate network.

2.4 Component of a communications network or service

For the purposes of this regulation, a-component of a communications network or service means a network element, device or information system which constitutes or utilises the communications network or service. The term is often used in Traficom's regulations. Components of a communications network or service include, for example, a mobile communications centre, a base station controller, a base station, an SMS centre, a broadband hub, a DNS server, a network access management server, a switch, a router, a SIP Application Server, a smart network component, a DVB-T network primary transmitter and gapfiller or a DVB-T2 transmitter. A component of a

[14] The concept of a separate network is used in section 244 a of the SVPL in a manner that differs from the repealed Communications Market Act (393/2003). In the Communications Market Act, a separate network was defined as a network that is not connected to a public communications network (section 130).

[15] As the justification for the regulation states, section 244 a, subsection 1 of the SVPL on public communications networks also applies to network services related to communications of public authorities in so far as it makes use of the public communications networks of telecommunications companies (HE 98/2020, p. 261).

[16] According to the preliminary work (HE 98/2020, p. 262), services critical to society have been identified based on, among others, the goals of a Government decision (VNp 1048/2018) adopted pursuant to section 2 of the Act on the Security of Supply (1390/1992) and as part of the national implementation of the Network and Information Security Directive (HE 192/2017).

communication-network or service does *not* refer to transmission links or parts of a device or network element, such as the CPU units in a mobile communication centre. If a function (e.g. DNS server software) has been decentralised in several devices, each device is considered to be a separate component.

2.5 4G network

For the purposes of this regulation, a 4G network refers to a mobile network (its core or radio access network) implemented using the LTE technology that is based on the EPS (Evolved Packet System) architecture defined in accordance with the technical specifications of 3GPP. An EPS consists of an Evolved Packet Core (EPC) and an Evolved UTRAN (E-UTRAN), optimised for-for packet switching traffic.[17]

2.6 5G network

For the purposes of this regulation, a 5G network refers to a mobile network realised using the fifth-generation technology that is based on the 5GC Fifth Generation Core Network (TS 21.905) or the New Radio (NR) fifth generation radio access technology in accordance with the technical specifications of 3GPP.

For the purpose of the application of the regulation, the concept of a 5G network also includes the 5G components of a 5G Non-Standalone (5G NSA) network, which therefore fall within the scope of the regulation's internal division of the critical parts of a 5G network. For example, if a component used in one part of a 5G network is defined as critical in the regulation, the definition also applies in a case where the component is being used as part of a 5G NSA network. During its lifecycle, a 5G NSA network will be upgraded to a 5G Standalone, or 5G SA,- network with full application of the definitions f the critical parts of a 5G network. It is not necessary to define 5G-NSA networks separately in the regulation, as they use the 4G and 5G network functions.

2.7 Concepts defined in section 3 of the SVPL

Otherwise, the definitions laid down in section 3 of the SVPL apply. The section defines at least the following concepts used in the regulation: telecommunications company, communication service, communications network, communications network equipment/device, public telephone service and public communications network.

3 Identification and documentation of critical parts of the communications network

3.1 Obligation to identify and document the telecommunications company and separate network operator

The first subsection of the section obliges telecommunications companies and separate network operators to identify the critical parts of their communications networks and the components of -the communications network or service they use with them. This means that they have to determine for their own networks which parts and components used therein they consider to be critical parts of the network based on the law and the regulation. A telecommunications operator and a private network operator must produce and keep up-to-date documentation on the critical parts of its communications network it has identified and on the components of the communications network or

[17] TS 21.905 Vocabulary for 3GPP Specifications.

service -used with them. The documentation must also indicate the criteria used by the telecommunications operator or separate network operator to regard the part of the communications network in question as critical.

As a component used with the critical part of the communications network, the documentation must include its identification data, such as the manufacturer, name and model number and software version, or other information. Once again, the documentation must give the criteria for regarding the part as critical, in which case it is possible to refer to the criteria set out in the regulation. In addition, the Regulation of the Finnish Transport and Communications Agency on information security in telecommunications (TRAFICOM/248815/03.04.05.00/2022) and the Regulation of the Finnish Transport and Communications Agency on the verification of communications networks and services and on the synchronisation of communications networks (TRAFICOM/54045/03.04.05.00/2020) set forth the requirements governing the documentation and other requirements related to the access rights of components and the access management of their equipment facilities.

The regulation states that the telecommunications company and the separate network operator should first identify the tangible network equipment they use with the critical parts of their communications networks. With virtualisation, for example, at least the components that are used to realise the physical virtualisation platform, the virtualisation infrastructure, the virtualised network functions and the management of virtualisation should be documented (cf. point 11 in the list in section 4 of the regulation). Secondly, the critical parts should also be identified in relation to the network architecture so that the company identifies and defines specific parts of its network as critical already at the network architecture planning stage, in which case the definition would guide the company to take into account the requirements of section 244 a of the SVPL when planning network device procurement. The assessment would have to be kept up to date in connection with changes made to the network architecture, security architecture or equipment base and when planning changes to them.

The identification of the critical parts of the network does not oblige the telecommunications company or separate network operator to assess their relevance to national security. In addition to the regulation, the operator must directly apply the definition in section 244 a(1) of the SVPL, according to which essential parts of the network functions and functions which essentially control or manage access to the network and traffic in the network are considered critical parts of the communications network.

The obligation in section 3 of the regulation is intended to promote the implementation of section 244 a of the SVPL and to ensure the uniform application of both it and the regulation. But for such a documentation obligation, Traficom would not be able to oversee as effectively compliance with the new rules by telecommunications companies and separate network operators. Traficom may, as part of its exercise of oversight, request the necessary documentation under its general right of access pursuant to section 315 of the SVPL.

The telecommunications company and separate network operator must independently assess the criticality of the parts of their communications network pursuant to the obligation to identify and document thus as provided in this section. Irrespective of the self-assessment made by the telecommunications company or separate network operator, Traficom will ultimately determine in

connection with its oversight whether a specific part of the network is to be considered critical.

3.2 Assessment of the criticality of 4G base stations in a separate network

The third subsection of the section imposes a specific obligation on a separate network operator to produce and keep an assessment of whether the base stations in its separate network are to be regarded as critical parts of the communications network. In practice, the assessment concerns base stations other than 5G network base stations, since 5G network base stations are always critical parts of the communications network under section 6 of the regulation. In its assessment, it must take into account at least the geographical coverage of the separate network, the share the individual base station has of the network traffic, and the functions and procedures implemented by the base station in the separate network. In addition to the separately mentioned criteria, any other factors relevant to determining whether access to the network or network traffic is essentially controlled or managed by the base station must be assessed. The obligation to keep the assessment means that it had to be checked to ensure that it is up to date and if necessary, amended if there are major changes to the network or in its use.

Traficom believes there are good arguments for also imposing the identification and documentation obligation on critical separate networks with respect to base stations other than 5G network base stations, as with them the network and its base stations may serve a small area, the service may be of great importance to its users and the base station functions may well be located more often on the same platform as the core functions of the network. However, Traficom has not considered it necessary always to determine base stations in all separate networks as critical parts of the communications network or to seek to establish any binding criteria for the related assessment.

The subsection also imposes a specific obligation on the separate network operator to document how it has arrived at its assessment. The obligation is also applicable if the operator decides that the base station (other than a 5G base stations) is not a critical part of its separate network.

The identification and documentation obligation for separate network operators does not apply to base stations or other parts of a communications network, or the components of the communications network or service used therein, where they are being used *for public telecommunications.* Obligations imposed on telecommunications companies applicable to parts of a public communications network.

4 Critical parts of a communications network

4.1 Definition of critical parts

This section determines the network features that must, at a minimum, be regarded as critical parts of a communications network. The list is not exhaustive, and the telecommunications company or separate network operator must also judge whether there are any critical parts in its communications network that are not listed here. Hence, the regulation does not limit the direct application of the definition of a critical part of a communications network in section 244 a(1) of the SVPL. The list in this section and the network technology-specific sections of the regulation complement each other.

The list is technology-neutral. As a rule, the section applies to all communications networks, such as circuit-switched and packet switching mobile networks and fixed broadband networks. The list has been drawn up primarily for targeted communications networks but it can also be used, where applicable, for the definition of the critical elements of a mass-communications network. Under the section, a part of a network is critical even if it only realises part of a feature that has been defined as critical. However, this approach to the definition and the approach based on a feature/functionality would lead to a situation where in a case where a single component can be shown to realise even part of a feature defined as a critical part of a network, the component would have to be considered a critical part of the network even if it did not implement the entire function. A single software component or network device can also implement more than one feature.

In addition to core network functions, the EU's toolbox[18] determines as critical the management of network virtualisation (NFV management) and Management and Network Orchestration (MANO) which are also included in the list in the regulation. With some qualifications, the list also includes invoicing, control and support systems other than MANO, transfer and transmission functions and interconnection points between networks, defined in the toolbox at a moderate/high level of criticality.

4.2 Critical features of the communications network

1) Traffic routing and other control or management of end user traffic

According to this subsection, the critical parts of a communications network include essential functions related to routing and other control or management of end user traffic in the communications network that may have a material impact on traffic in the communications network. The subsection also states specifically that the critical parts of a communications network on this basis include at least the following:

i. components -of a public communications network or service in priority categories 1 or 2 pursuant to the Regulation on the verification of communications networks and services and synchronisation of communications;

ii. components -components of a communications network or service, where they otherwise control or direct a substantial part of traffic throughout the network;

iii. components of a communications network or service in the data centre network, when they are vital for the operation of a critical part of the communications network;

iv. components of a communications network or service transmitting or routing traffic between critical parts of a communications network in priority category 3 in the Regulation on the verification of communications networks and services and on the synchronisation of communications networks.

[18] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. Annex 2, p. 39. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures. See also EU coordinated risk assessment of the cybersecurity of 5G networks. Report. 9 October 2019, k. 2.21. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049.

This subsection therefore covers the key functions of the network that ensure the routing or other control of end user traffic in the network to terminal devices and between networks. The subsection also includes corresponding functions related to M2M traffic. In addition, the subsection includes systems capable of analysing the traffic of users that are used to detect harmful traffic and that may also be covered by the later section on information security functions.

As regards mobile communications networks, this subsection covers, in particular, features related to the transmission of the user plane or features used to control network traffic through the control plane. It also includes mobility management in mobile networks. In the case of mobile communications networks, the Short Message Service Centre (SMSC) and the connected gateways also control the traffic of users in the manner referred to in this subsection.

This subsection also covers features pertaining to network slicing in so far as they realise functions in accordance with the section. Network slicing refers to the grouping and unbundling of traffic in a mobile communications network in order to guarantee the desired quality parameters. A network slice forms a logical whole (a logical network) in one physical network infrastructure. A network slice may have common and dedicated resources. In the mobile communications network, the fourth and fifth generation technologies support network slicing to different extents and in 5G, several network functions are involved in slicing.

These functions are used to control and manage traffic in the network, which is why they must be regarded as critical parts of the communications network. The functions are also essential to ensure the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

In particular, the core network is essential for the control of network traffic and for the availability of services, as the network’s traffic is routed or transmitted through it. For the same reason, the backbone network is also crucial for the confidentiality of communications. On a similar basis, the components of the regional and transmission system may also be essential, since without them traffic between base stations and the core network would not be a possibility. Therefore, components transmitting and routing traffic between critical parts of a communications network should also be regarded as critical parts of the network, at least when they are in priority category 3 in the Regulation on the verification of communications networks and services and the synchronisation of communications networks.

The subsection also specifies that the critical parts of a public communications network include components of a communications network or service in priority categories 1-and 2, including border routers meeting this criterion, regardless of whether they form part of the core, regional or transmission network in the operator’s architecture. Priority classification is currently stipulated in the Regulation on the verification of communications networks and services and on the synchronisation of communications networks. The obligation regarding priority in this regulation does not apply to separate networks. Network devices belonging to these priority categories are always critical parts of a communications network because they affect such a significant number of users that they must always be regarded as controlling or essentially controlling network traffic.

In addition, as indicated by a second specification, critical parts of a communications network include any components that control an essential part of all the communications network's traffic. This also applies to separate networks. These include, for example, central components of the backbone network. A backbone network can be used to transmit traffic of both a mobile network and a fixed network. All or most of the traffic between base stations and the mobile network core, or the traffic within the core or the fixed network traffic, is transmitted or controlled in the backbone network. The backbone network connects regional networks to one another. An example of the parts of a network covered by this subsection is an IP/MPLS network connecting an operator's regional networks. However, the application of this subsection is not limited to the backbone network or the core network, as the definition of these is not unambiguous.

A third specification indicates that a data centre network is also covered by this subsection when, for example, it connects critical parts of a communications network produced in the data centre, such as the core functions of a mobile network, to the backbone network.

A fourth specification indicates that the critical parts of a communications network will in future also include components in priority category 3 when they transmit or route traffic between the critical parts of the communications networks.

2) End user access management, authentication and authorisation, allocation of network resources to end users, and end user connection and session management

This subsection covers functions which manage the access of end users, and thus the terminal devices used by the end users, to the network, maintain user sessions and the status of connections, verify and authorise end users (terminal devices) and ensure the allocation of network resources to them. The authentication of users, the distribution of network resources to users and the management of user sessions are essential not only for the availability of the service but also for the maintenance of the confidentiality of communications.

This subsection covers, for example, features which in mobile networks verify the user's terminal device, transmit the verification between networks and enable bearer management between the terminal device and the network. The section also covers mobility management in mobile networks.

As regards mobile networks, this subsection also covers the authentication of connections from different networks in a centralised component (Non-3GPP Access) and the Authentication, Authorisation and Accounting (AAA) feature, where it relates to the authentication and authorisation of end users.

Regarding resource allocation, the subsection covers, for example, the allocation of IP addresses to the users' terminal devices and DNS servers serving the users, which are crucial for the availability of the service.

It also covers features pertaining to network slicing in so far as they realise functions mentioned in the section, such as the assignment of terminal devices to the network slices. In 5G, a number of network functions are involved in slicing. Key security risks associated with slicing include insufficient slice unbundling and access management, in which case there is a risk of data

leakage between slices or the retention of the shared computing power of the slices.

These functions specifically control and manage users' access to the network, which is why they must be regarded as critical parts of the communications network. The functions are also crucial for the control of network traffic, the maintenance of connections and assurance of the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

3) Registration, authentication and authorisation of communications network and service functions;

Under this subsection, the critical parts of a communications network include the registration and mutual authentication and authorisation of the various functions within the network. The critical parts of a communications network include, for example, various network registers that would maintain information on network functions and network functions that would authorise other functions (Authentication, Authorisation and Accounting or AAA).

These functions are used to control and manage access to the network, such as the access of the different network functions, which is why they must be regarded as critical parts of the communications network. The functions are also crucial for the control of the network, the control of the access of users to the network, the maintenance of connections and assurance of the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

4) Infrastructure-services needed to support the operation of a communications network and communication service

Under this subsection, the critical parts of a communications network include the infrastructure services necessary for the operation of the communications network and communication service. Such functions include:

- repositories containing information on critical network functions and user data
- internal address assignment and name services in the network core serving the network components, such as DNS and DHCP services
- time services used in critical parts of the network for synchronisation of time (these influence key management and logs, for example)
- a centralised time service system that transmits and ensures the time and phase synchronisation signal of base stations[19]

These functions are used to control and manage the access of different functions of the network to the network and the synchronisation traffic in the network, which is why they must be regarded as critical parts of the communications network. The functions are also crucial for the control of the network, the control of the access of users to the network, the maintenance of connections and assurance of the availability of services, the confidentiality of com-

[19] Including at least ePRTC (Enhanced Primary Reference Time Clock), T-GM (Telecom Grandmaster) and the atomic clock. The same system may be able to transmit centrally to the base stations a synchronisation signal provided through a satellite positioning system under normal conditions, in addition to verification. This system does not refer to the transmission system components used to transmit a signal, which are typically the same as for other data traffic and which may be critical parts of the communications network based on other sections of this regulation.

munications and the information security of the communications network as a whole.

5) Functions implementing interfaces between communications networks or services, including roaming

According to this-subsection, functions that implement interfaces between the communications network or service and other communications networks and services are critical parts of a communications network. This refers, in particular, to external interfaces of the network core which provide access to the network services from other networks or services that may be either networks or services of the telecommunications company or separate network operator, or networks or services provided by another operator.

The critical parts of a communications network also include roaming interfaces that are open, for example, to IPX operators to enable network-to-network connections. The interfaces referred to here can also enable access to the network features via a wireless local area network, for instance. An internet gateway for the users of the network, as well as interfaces with other internal systems of a telecommunications company or a separate network operator, such as an IMS network, are also considered to be critical parts of the communications network.

External interfaces may enable intrusion into the functions of the core network to undermine the performance of the network or to obtain confidential information about the network functions and its users. There is a variety of interface implementation methods, and many of their security features remain outside the scope of standardisation.

These functions are used to control and manage traffic in the network and the access of services to the network, which is why they must be regarded as critical parts of the communications network. The functions are also crucial for the control of the network, the control of the access of users to the network, the maintenance of connections and assurance of the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

6) Functions interconnecting communications networks or services when the function may have a material impact on access to the communications network or on traffic passing through the network;

This subsection covers internet exchange points and direct interconnection with other networks and services, with the traffic being transmitted between communications networks. In addition to the IP backbone network, IP transit and routing points to the networks of other operators and the internet are crucial in terms of the communications network and the performance of the services therein. The material impact of interconnection on communications network traffic would be assessed in relation to traffic of the type in question in the network.

This subsection covers, for example, the internet exchange point (IXP) and the mobile operator exchange point (DIX). The link to the exchange point may be part of the operator’s backbone network, the components of which would be critical parts of the communications network. according to the criteria in subsection 1.

These functions are used to control and manage traffic in the network, which is why they must be regarded as critical parts of the communications network. The functions are essentially related to the availability of traffic and services between networks and to ensuring the confidentiality of communications and the information security of the communications network as a whole.

7) Centralised management of a communications network and related functions, the encryption of end user traffic and keys

This subsection covers centralised functions related to the establishment, retention, transmission, integrity and other lifecycle stages of communications network devices, software and users' encryption keys. A function can be considered centralised even if it is physically distributed among several places where equipment is kept, for example. The section also covers functions involved in the certificate hierarchy and/or that are used to create and transmit keys as well as transmit their validity data (Certificate Revocation List or CRL, or equivalent).

This subsection applies not only to authentication and encryption between users and the network, but also between network components and network functions.

This subsection covers the following areas in particular: encryption of traffic between network base stations and the core of the network (including base stations' wireless transmission links), encryption used by backbone network components and encryption of core functions. It also covers encryption of data warehouses used by the critical parts of the communications network.

These functions are used to control and manage user traffic in the network and users' access to the network, which is why they must be regarded as critical parts of the communications network. The functions are essential for the confidentiality of communications and the information security of the communications network as a whole.

8) Information security functions affecting critical parts of a communications network

This subsection covers functions which are used to monitor, control, limit or filter network traffic or process log data for systems associated with the critical parts of the communications network. This subsection also covers functions that are used to manage and supervise procedures relating to the maintenance or management of the network.

Information security functions protect the core network from threats from the direction of the radio network and external networks, as well as the functions of the core network against internal threats. Information security functions, such as security software on servers, enable the control of critical system platforms or their operating systems. This subsection also covers information security functions targeting other critical parts of the communications network, such as management connections.

The information security function to protect the core of the network referred to in this subsection may also have been implemented outside the core network from the perspective of the network architecture. This subsection also covers other information security functions affecting the critical parts of the communications network, such as control systems.

Information security functions separate the different security zones and segments of the network, and filter and control traffic between them. These include:

- segments between the network core and the transmission system and the radio network; and

- interfaces between OSS and BSS systems and their interfaces with the communications network; and

- functions meant to monitor and control traffic between or within the above, such as firewalls, are terminating Security Gateways and Border Gateways between the different security domains of a tunnelled traffic operator's network that are used to control and manage traffic between the different networks of a single operator or the networks of different operators.

Information security functions can also be Network Functions Virtualisations (NFVs) that virtually provide network services and software. They can share a platform with other similar software.

This subsection covers information security functions for controlling and transmitting network services to external networks, such as roaming networks or other networks outside the mobile network. Examples include Diameter Edge Agent and, in the case of a 5G network, the SEPP (Security Edge Protection Proxy) gateway that acts as an intermediary for the implementation of traffic and services between the networks of different operators and protects the communications of the network core services in the direction of the link between the operators. Other examples of information security functions that may also be virtualised include network security software such as firewalls, traffic filtering software or network infrastructure support software, e.g. DHCP or DNS services.

These functions are used to control and manage traffic in the network and access to the network, which is why they must be regarded as critical parts of the communications network. The functions are essential for the confidentiality of communications and the information security of the communications network as a whole.

9) Network management and surveillance systems and other specific invoicing, supporting and back-end systems

Under this subsection, network management and network surveillance systems are critical components of the communications network. The subsection further specifies that the critical parts of the communications network include at least:

i. systems for the management or surveillance of critical parts of the communications network;

ii. systems that materially affect access to the network or traffic passing through the network;

iii. billing, support and back-end systems that may materially affect access to the communications network or traffic passing through the network; and

iv. network management and surveillance systems for the components routing or transmitting traffic in critical parts of the communications network.

Network management and surveillance systems are therefore critical parts of a communications network firstly when they are connected to the management or control of a function considered to be a critical part of the communications network for other reasons. Secondly, the functions referred to herein are critical parts of a communications network when they may otherwise have a material impact on access to the communications network or the network traffic due to, for example, the number of controlled elements, even though a single controllable element is not a critical part of the communications network. For example, 2G or 4G network base station management systems may be a critical part of a communications network on this basis even if a single 2G or 4G network base station itself would not be considered a critical part of the a communications network. This is because base station management system can affect and even entirely block users' access to the network as well as the traffic transmitted by the base stations, for example by slowing it down.

Here, network control and supervision systems refer to software, equipment or interfaces that are used to operate, maintain or otherwise manage and control the various resources of a communications network, such as base stations, information security systems, network devices and software used for network maintenance.

Network control and supervision systems include OSS (Operations Support Systems) and MANO (Management and Orchestration) systems, as well as their interfaces with BSS (Business Support Systems). OSSs and BSSs can be interconnected, depending on the network architecture, by means of a gateway, which then forms an interface that is considered critical. Automatic systems used for network optimisation and control may also be covered by this subsection in whole or in part based on these requirements. These include systems that collect data on the performance of the network and control the network by, for example, supplying analysed network data back to the network functions. This subsection also covers, for example, IPAM systems that manage address assignment in the network and the systems referred to in section 4(2) of Regulation 66 A/2019 M of the Finnish Transport and Communications Agency of 2 December 2019 on disturbances in telecommunications for receiving and analysing the surveillance data of a communications network or service.

MANO features include the NFV orchestration components of a software-controlled network, for example. Their main tasks are to control, define and harmonise the connections between network components in software-controlled networks. The features covered by this subsection also include VIM and VNF features that manage the virtual network infrastructure, including the platform and the related service components. Network slicing management would also be covered under this section. Software Defined Networking (SDN) is also covered by this subsection. SDN refers to the virtualisation of network functions and their transfer to a harmonised control level where the network features can be controlled through software interfaces. In the case of 5G networks, for example, management can be automated and the network controlled programmatically and dynamically in line with the changing needs.

In the case of other invoicing, support and back-end systems (e.g. BSS), the subsection covers systems that can be used materially to affect access to the communications network or network traffic, in terms of the availability of services, for example. For example, misuse or a software error could lead to a situation where systems that affect the provisioning of subscriptions could be used to exclude a large number of subscriptions from the network.

Here, 'invoicing system' refers to both functions related to the technical implementation of charges in the network core and invoicing support systems outside the core. Even though a network can operate without an invoicing system, invoicing can be considered a critical part of a communications network if it can have a material impact on the availability of services or the confidentiality of communications. Invoicing system functions can typically be divided into online and offline functions. In the case of mobile networks, network invoicing management and architecture are defined in the technical 3GPP specification 32.240. An invoicing system may affect the availability of a service in the case of online invoicing by blocking, in real time, a user's access to the network or its services through a quota management service, in which case it allows or denies the user access to the service on a time or data basis. The invoicing system collects and processes invoicing data that may contain information describing confidential information on the parties involved in the communication, for example. An invoicing system allows access to transmission data processed in the network, which may compromise the confidentiality of communications.

These functions are used to control and manage traffic in the network and access to the network, which is why they must be regarded as critical parts of the communications network. The functions are essential for the control and management of the network, control of the access of users to the network and ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole. Invoicing system functions can be used to control and manage access to the network, which is why they may be regarded as critical parts of the communications network. The functions are essentially related to the control of traffic in the network and to ensuring the availability of services, but also to the confidentiality of communications.

10) Implementation of interception or monitoring of telecommunications

Under this subsection, lawful interception (LI) features would be critical parts of a communications network. This subsection applies not only to components acquired separately for LI but also to other network components directly related to the implementation of the LI feature. The technical 3GPP specifications define functions that realise LI features.

This subsection contains the technical devices in, and characteristics of, a communications network and service required under point 16 of section 243(1) of the SVPL-and section 245 of the SVPL that a telecommunications company uses to ensure the fulfilment of the technical and operational requirements for the monitoring and interception of telecommunications (see HE 221/2013 p 183–184 and p 187).

Correct performance of these functions is essential for the confidentiality of communications. Depending on the procedure, they are linked at least to traffic control (recording of telecommunications interception data), user access management (potential for temporarily blocking the use of an address

or equipment as a component of the monitoring of telecommunications; section 10(6) of the Coercive Measures Act, 806/2011) or other network access (access to telecommunications monitoring and interception data).

11) Virtualisation when it is used to implement a function or procedure considered a critical part of a communications network

This subsection defines virtualisation as a critical part of a communications network when features of the critical parts of the communications network are being virtualised. In such a case, the virtualisation platform (the virtualisation infrastructure and its physical platform) controls components, which in turn control and manage the network and the traffic passing through it, and is thus a critical part of the communications network. In a virtualised communications network, the network functions are dependent on the virtualisation platform and its management and orchestration systems.

The critical parts of the communications network covered by the section on virtualisation are largely defined in the other sections of the regulation. As the regulation is not exhaustive, the critical parts of a communications network may, pursuant to section 244 a of the SVPL, also include parts other than the critical parts of a communications network specified in this regulation. Section 3 of the regulation obliges a telecommunications company or separate network operator to identify the critical parts of its communications network. The section on virtualisation would therefore in principle mean that the virtualisation of the critical parts of the communications network identified by the telecommunications company would also be a critical part of the communications network.

The subsection does not state that virtualisation is critical as such. In a case where only functions and procedures not considered to be critical parts of the communications network are virtualised, the virtualisation would not be considered a critical part of the communications network either.

The core of a 5G network is based on virtualised services that can be produced in environments which resemble a typical IT infrastructure, but the network functions of the previous generations can also be virtualised. In a 5G network, the actual network functions can be virtualised, networks can be controlled by software and network capacity can be divided into virtual slices according to different needs. Network Function Virtualisation (NFV) refers to the implementation of 5G network functions programmatically instead of with traditional network equipment. Virtualisation platforms can be shared between several functions or software products. The security of the platforms becomes a critical factor in ensuring the information security of the entire network.[20] One or more network functions can be implemented on a virtualisation platform.

According to the criteria set out in the subsection, the critical parts of a communications network could include at least Virtual Network Functions (VNF), the Network Functions Virtualisation Infrastructure (NFVI), the management and orchestration of virtualised functions and virtualisation, and the physical virtualisation platform. The management of virtualised functions and virtualisation is realised with a MANO system, which includes at least the NFV Orchestrator (NFVO, which manages e.g. the orchestration of resources between VIMs), the VNF Manager (VNFM, which manages VNF instances) and

[20] For information on security threats linked to virtualisation, see e.g. 3GPP TR 33.848 V0.5.0 (2019-11). Study on Security Impacts of Virtualisation. https://www.3gpp.org/DynaReport/33848.htm.

the Virtualised Infrastructure Manager (VIM, controlling the virtualisation infrastructure or NFVI).[21]

12) Features implemented through virtualisation that is considered a critical part of the communications network

Under this subsection, a function or procedure other than those mentioned above or otherwise considered a critical part of a communications network is regarded as a critical part of a communications network when it is realised by means of virtualisation that is considered a critical part of the communications network pursuant to point 11 in this list. The previous subsection defines virtualisation itself as a critical part of a communications network in certain situations. When virtualisation is considered a critical part of the communications network, this subsection defines other features implemented in the same virtualisation environment as critical parts of the communications network.

When virtualised functions share resources, information security risks and dependencies between virtualised functions arise, and the functions may be able to influence other virtualised functions. Access to the platform from a virtualised function would compromise the other functions. For this reason, it is justified to consider all functions realised on the same critical virtualisation platform as critical parts of the network and regard them as being used in a critical part of the communications network, even if some of them are not critical parts of the communications network when realised on a separate platform.

This subsection does not as such prevent the realisation of critical and otherwise non-critical functions on the same platform: instead, the realisation on the same virtualisation platform will allow the virtualised functions otherwise considered non-critical to fall within the scope of application of section 244 a. It is possible for a telecommunications company to realise the functions on the same platform provided that, in so doing, it will still be able to meet its obligations under other rules.

13) Key functions and procedures to allow access to data on the geographical location of a subscription or terminal device processed in a communications network or data that enables the location to be determined by means of the communications network

Data revealing the geographical location of the subscription or terminal device and thus the user's geographical location (geographical information) is a potential area of misuse and may even expose users to physical threats. These may consist of transmission data which is normally processed for the transmission of communication and which also reveals the location of the user with a certain degree of accuracy, or geographical information that is processed for purposes other than the transmission of communication. Geopositioning services/components in a network are not always directly connected to the transmission of communications; instead, they can be used for 'added value services' and may therefore not be fully covered by the subsections above. The concepts of transmission data, geographical information and value added service are defined in section 3 of the SVPL.

Under this subsection, critical parts of a communications network would include firstly functions and procedures that allow access to data on the geo-

[21] For more information on virtualisation in a 5G network, ENISA Threat Landscape for 5G Networks, s. 3.7. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

graphical location of a subscription or terminal device in a communications network, such as transmission data or geographical information stored there. These functions can be seen as controlling or managing access to the network, which is why they must be regarded as critical parts of the communications network. Secondly, critical parts of a communications network would include functions and procedures that enable the determination of the geographical location of a subscription or terminal device. The determination of location can be understood to be based on the control of the network and its traffic.

Functions referred to in the subsection would include:

- Gateway Mobile Location Centre (GMLC), which supports the provision of location-based services and allows functions authorised to use the data or external service providers, such as a provider of an added value service that processes data with the user's consent, to enquire regarding the user's location and grants them access to geographical information (3GPP TS 23.273, Rel.) 16).

- Enhanced Serving Mobile Location Center (E-SMLC), which supports the determination of the location of a terminal device in an LTE network (3GPP TS 23.271), and

- Location Management Function (LMF), which supports the determination of the location of a terminal device in a 5G network (3GPP TS 23.273)

These functions are used in, for example, emergency positioning.[22] Several other functions that have been determined as critical either in the subsections above or hereinafter in other sections of this regulation, are involved in the implementation of location-based network services.

5 Critical parts of the 4G network

5.1 Definition of the critical parts of a 4G network

This section defines the network features that at the very least are critical parts of a 4G network by referring to the core features in technical specification TS 23.002 of the 3rd Generation Partnership Project (3GPP). The first subsection of this section is largely a clarification, based on the premise that core features are critical parts of a communications network.

The first subsection stipulates that, in the case of the functions and procedures in the core of a 4G network, the critical parts of a communications network are the packet switching features under sections 4.1.1, 4.1.4 and 4.1.5 of the 3GPP technical specification TS 23.002 in so far as they essentially control or manage access to the network and the traffic in the network. Therefore, not all the features included in these sections are necessarily critical parts of a communications network. The clarification regarding 'packet switching' in the first subsection is intended to exclude all circuit-switched features included in the above-mentioned sections[23]. The features may have also been defined in the manner intended in the section in technical specification 23.002 by referencing the other 3GPP specifications.

[22] Network Induced Location Request (NI-LR). 3GPP TS 23.273, see 6.10.1 (5GC-NI-LR Procedure).

[23] E.g. SMS-GMSC (SMS Gateway MSC) and SMS Interworking MSC (SMS-IWMSC), which are connected to the delivery of text messages to base stations or from base stations to the SMS centre.

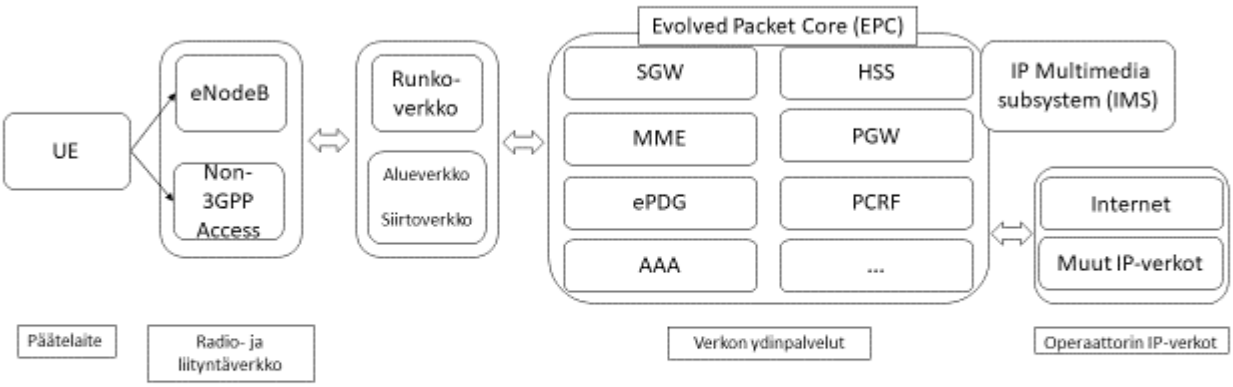
The second subsection of this section determines the 4G network features that must, at a minimum, be regarded as critical parts of a communications network. In the case of the features mentioned in Table 1 in the regulation, a more detailed analysis of the criticality of the part of a communications network would not be necessary; instead, these should be considered by default as critical parts of the communications network.

The first subsection and the table of critical parts referenced in the second subsection are not exhaustive in any respect: the telecommunications company or separate network operator must also judge whether there are other critical parts in its network in addition to those mentioned in the table. The list should therefore be accompanied by a definition of the critical parts common to all networks in section 4 of the regulation and the definition of the critical parts of a communications network in section 244 a(1) of the SVPL as such.

Functions (features) according to the 3GPP specifications are logical and distributed among several applications. According to the section, a part of a network would be critical even if it only implemented part of a feature that has been defined as critical. This approach and the approach based on a feature would lead to a situation where in a case where a single component can be shown to implement even part of a feature defined as a critical part of a network, the component would have to be considered a critical part of the network even if it did not implement the entire feature. A single software component or network device can also implement more than one feature.

It should be clear that, in the case of 5G NSA networks, the criticality of the 4G network components used would, as a general rule, be assessed according to what is stipulated for 4G network parts in the regulation. The 5G-NSA network is based on the EPC core of the 4G network. For the purposes of this regulation, the list of critical parts of a 4G network also applies to 4G network functions used by a 5G NSA network.

Figure 1 illustrates a communications network architecture based on LTE technology at a general level. The ‘IP Multimedia Subsystem’ mentioned in the figure is dealt with in section 7 of the regulation. All the features described below are part of the core network services shown in the figure.



Runkoverkko, Alueverkko Siirtoverkko	Backbone network, Regional network, Transmission network
Muut IP verkot	Other IP networks
Päätelaite, Radio- ja liityntä verkko, Verkon ydinpalvelut, Operaattorin IP-verkot	Terminal equipment, Radio and Access Network, Network Core Services, Operator's IP networks

Kuva 1 An example of a 4G network architecture at a general level

When list 1 in the regulation was drawn up, a similar list prepared in the United Kingdom was used as a reference point. In the United Kingdom, a circular from the National Cyber Security Centre (NCSC) drew the attention of telecommunications companies in addition to 5G networks to certain functions of 4G networks and certain functions that involve a particularly high risk in all networks.[24]

5.2 Critical features of a 4G network

Home Subscriber Server (HSS)

Home Subscriber Server (HSS) is a central database that contains data for handling user sessions and connections in a communications network based on the LTE technology. A mobile network may have one or several central databases, depending on the number of users and the architecture of the network.

The HSS handles user access management, user identification, user profiles and mobility management, e.g. by providing information on the MME serving the user. The HSS also handles key management and the creation of user and communications network authentication vectors. The HSS also plays a role in the implementation of the interception and monitoring of telecommunications (Lawful Interception or LI features).

According to the 3GPP technical specifications, HSS currently includes the Home Location Register (HLR) and the Authentication Centre (AUC) features.[25]

This function controls and manages users' access to the network, which is why it must be regarded as a critical part of the communications network. The function is also essential for the control of the communications network and its traffic, the maintenance of connections and ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Equipment Identity Register (EIF)

The EIF is a mobile network database that stores International Mobile Equipment Identities (IMEIs) and includes information on the authorisation to use mobile phones. Normal use of terminal devices included in the EIR blacklist in a communications network is not allowed.

[24] NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, section 11.a. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks; see also section 12. In the case of 4G, these functions are: "mobile core functions, including Home Subscriber Server (HSS), Packet Gateway (PGW), Policy and Charging Rules Function (PCRF) and, in some cases, the Mobility Management Entity (MME) and Serving Gateway (SGW)".

[25] 3GPP TS 23.002, see 4.1.1.1.1–4.1.1.1.2.

This function controls users' access to the network, which is why it must be regarded as a critical part of a communications network. The function is linked to the prevention of the use of unauthorised devices in a network and is therefore essential for ensuring the availability of network services.

Subscription Locator Function (SLF)

The SLF transmits the name of the central database containing user data (HSS) to the network functions (AAA, AS, I-CSCF) if there are more than one of them in the mobile network.

This function controls and manages users' access to the network services, which is why it must be regarded as a critical part of a communications network. The function is also essential for the control of the communications network and its traffic, the maintenance of connections and ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Mobile Management Entity (MME)

The MME controls the termination of the terminal device control plane, the registration of terminal devices, the management of connections and mobility management. It also plays a role in roaming. The MME also implements LI features.

This function controls and manages users' access to the network, which is why it must be regarded as a critical part of the communications network. The function is also essential for the control of the communications network and its traffic, the maintenance of connections and ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Serving Gateway (SGW)

The SGW controls user-level traffic routing and management between base stations and the PDN-GW. The MME controls the SGW for the creation of new connections and the modification of existing connections between the terminal device and the network. The SGW also implements LI features.

This function controls and manages network traffic, which is why it must be regarded as a critical part of a communications network. The function is also essential for maintaining connections and ensuring the availability of services and the confidentiality communications in a communications network.

Packet Data Network Gateway (PDN GW)

The PDN-GW is an interface function between the operator's internal IP network and an external IP network. PDW-GW is allocates IP addresses to terminal devices. It also monitors acceptable use policy. In addition, the PDN-GW performs traffic filtering and analysis, which enable invoicing and the control of traffic. The PDN-GW also implements LI features.

This function controls and manages network traffic, which is why it must be regarded as a critical part of a communications network. The function is also essential for maintaining connections and ensuring the availability of services and the confidentiality communications in a communications network.

Evolved Packet Data Gateway (ePDG)

The ePDG is used to establish a connection between non-3GPP access users by routing traffic between the PDN-GW and the user. The EPDG is usually used to realise the VoWiFi service (Voice over Wi-Fi, a wireless call service via a local area network).

The ePDG will activate the key exchange between the user and ePDG and establish an IPSec tunnel to secure communication at the interface. The ePDG also carries out authentication and authorisation of the IPSec tunnel as well as implementing LI functionalities.

This function controls and manages network traffic, which is why it must be regarded as a critical part of a communications network. The function is also essential for maintaining connections and ensuring the availability of services and the confidentiality communications in a communications network.

3GPP AAA Server and 3GPP AAA Proxy

The AAA server controls the authentication, authorisation and mobility of non-3GPP access users and includes the necessary user data to implement access management. The AAA proxy provides the corresponding services during roaming. When necessary, the AAA proxy selects the gateway serving the user's session.

The AAA server is particularly related to the implementation of the VoWifi service. The AAA also implements LI features.

This function controls users' access to the network, which is why it must be regarded as a critical part of the communications network. The function is also essential for the confidentiality of communications, the control and management of the communications network and its traffic, and the maintenance of connections.

Access Network Discovery and Selection Function (ANDSF)

The ANDSF is manages for user traffic control between a mobile network and non-3GPP access networks, such as a WLAN network, sharing data for traffic routing and terminal device mobility. Depending on the implementation method, the data is either retrieved from the ANDSF server or distributed by the server among the target devices.

This function controls and manages user traffic in the network, which is why it must be regarded as a critical part of a communications network. This function is also essential for users' access to the network and the availability of network services.

Policy and Charging Rules Function (PCRF)

The PCRF serves as a control point for user connections and invoicing. It ensures that user-level traffic conforms to the user profile. The PCRF plays a key role in controlling the quality of the service, invoicing, VoLTE voice service and roaming.

This function controls and manages user traffic and access to the network, which is why it must be regarded as a critical part of a communications network. The function is also essential for the maintenance of connections and ensuring the availability of services.

6 Critical parts of the 5G network

6.1 Features of a 5G network and its architecture

The core of a 5G network consists of certain core functions in a network without which the network will not be able to operate or provide certain critical services for the network. It also consists of interfaces with external systems and networks, the edge network and external IPX and data network functions. At the core of the network, decisions are made on the user's access to the network and on traffic control, and whether the data will be directed to be processed locally in the network close to the user. Controls and decisions regarding the infrastructure required by the network and its platforms, and verification of the performance of the network also take place at the core of the network.

The core of a 5G network is based on a gateway and software components. The platform and the network's software-based components are separated at the core of the network, and they can be built independently of each other. Several functions or software products can share the platform. The security of platforms is a critical factor in ensuring the information security of the entire network. Risks involving the network core functions include external interfaces that can be used to influence or infiltrate the core software, as well as transverse traffic within the network core. In a 5G service architecture, standardised gateways enable fixed integration of service providers into the important 5G core gateways. This enables the network to adapt in such a way as to optimise the network for the services used by users.

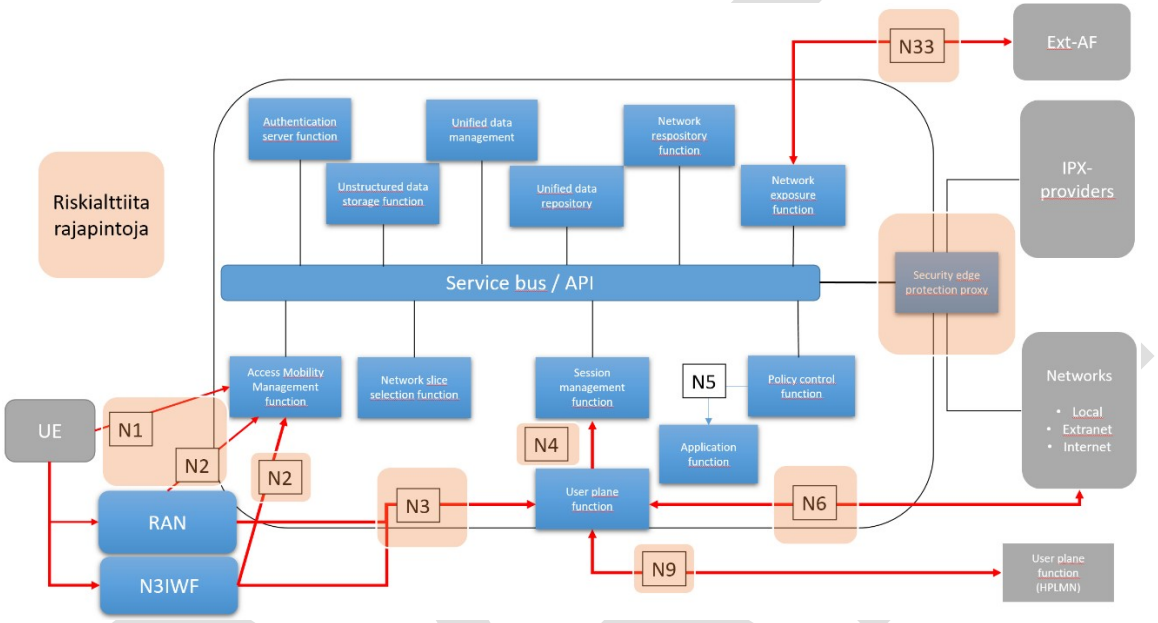
Components that control the operation of a 5G network are treated as network functions that can consist of multiple software products or 'containers' and provide a standardised and complete environment for the necessary software. Traffic between the core functions of the network takes place along a standardised gateway. The network core also provides interfaces that enable users' roaming in a network of another operator, as well as traffic to other networks, such as the internet or the internal networks of organisations.

In 5G networks, virtualisation is the main way to implement the functions of the core network, and virtual environments are also becoming significantly more dynamic, allowing services to be scaled according to the number of users and their needs. Virtualisation can also be used in 4G technologies and the IMS. Platform solutions can be switched to cloud-based virtualisation solutions in telecommunications platforms and server platforms. Different components of the network, such as base station software and network core features, can be produced using virtualised platforms.

Components connected to the network base stations that provide traffic control and routing, user identification, authorisation, and the control and sharing of encryption keys can be considered parts of the core of a 5G network. The core also includes the telecommunications company's mobile network interconnection interfaces with the networks and applications of other operators. The corresponding functions in the 3GPP definition are at least UPF, AMF and SEPP, as well as the service-based architecture components associated with these components. The key functions of a 5G network, as defined by 3GPP architecture, are presented in Figure 2.

In general, the main security areas of a 5G network can be divided into two levels: the core of the network and its interfaces and the edge network. The

edge network includes network transmission links, regardless of how they are implemented, base stations and possibly edge computing components. The distinction between the core and the edge of the network is not unambiguous, but the boundary between them can be considered to consist of, on one hand, the N1 and N2 interfaces between the terminal devices and the base station control connection (the control plane) and the network, and on the other, the N3 interface between the base station and the network (user plane). Interfaces N32 and N6 separate the network from the IPX and data-based network and the N9 interface from the guest network.



Riskialttiita rajapintoja

High risk interfaces

Kuva 2 Key functions and interfaces of the 5G core network

6.2 Definition of critical parts of the 5G network

This section defines the network features that at the very least are critical parts of a 5G network by referring to the 3GPP technical specification TS 23.501.

The first subsection states that the critical parts of a communications network are the functions in a 5G network as defined in section 6.2 of the 3GPP technical specification 23.501 and in section 4.1 of 38.300 to the extent that they essentially control or manage network access and traffic passing through the network. Therefore, not all the features included in these sections are necessarily critical parts of a communications network. The features may have also been defined in the manner referred to in this section in technical specification 23.501 by referencing the other 3GPP specifications.

The second subsection of this section determines the 5G network features that must, at a minimum, be regarded as critical parts of a communications network. In the case of the features mentioned in Table 2 in the regulation, a more detailed analysis of the criticality of the part of a communications network would not be necessary; instead, these should be considered by default as critical parts of the communications network.

Functions (features) according to the 3GPP specifications are logical and distributed among several applications. According to the section, a part of a network would be critical even if it only implemented part of a feature that has been defined as critical. This approach and the approach based on a feature would lead to a situation where in a case where a single component can be shown to implement even part of a feature defined as a critical part of a network, the component would have to be considered a critical part of the network even if it did not implement the entire function. A single software component or network device can also implement more than one feature.

The 5G components of a 5G NSA -5G NSA network are covered by the definition of the critical parts of a 5G network in terms of the scope of application of the different parts of the regulation. For example, if a some of a 5G network is identified as critical, it is also critical in the context of a 5G NSA network. Similarly, in the case of 5G NSA networks, the criticality of the 4G network components used would be essentially assessed according to what is stipulated for 4G network parts in the regulation.

The first subsection and the table of critical parts referenced in the second subsection are not exhaustive in any respect: the telecommunications company or separate network operator must also assess whether there are other critical parts in its network in addition to those mentioned in the table. The list must therefore be accompanied by a definition of the critical parts common to all networks in section 4 of the regulation and the definition of the critical parts of a communications network in section 244 a(1) of the SVPL as such. As the table is not exhaustive, any other functions to be defined in the future that would implement a similar critical feature could be critical parts of the communications network, either pursuant to section 4 of the regulation or section 244 a(1) of the SVPL.

6.3 Critical features of a 5G network

Next generation Node B (gNB)

A gNB (base station) performs a number of key radio communication management tasks, including user network access, connectivity, disconnection and terminal mobility management.

The management and allocation of base station radio resources in the area affected is comprehensive and dynamic. The interface between base stations (Xn) significantly extends the reach of a single base station beyond its own coverage area.

The radio network has the ability to adapt and optimise connections automatically and in real time, for example by monitoring the traffic load of the base station and the area it affects, by collecting data on terminal equipment, by monitoring, by contributing to the prediction of the movement of terminal equipment and by analysing the quality of service both at the connection level and in general.

In terms of the protection of network traffic, the main functions of the base station are the packaging of the IP and ethernet frames, traffic unloading, encryption and integrity protection. The gNB also routes user and control traffic to the components of the mobile network core.

This function controls and manages users’ access to the network, which is why it must be regarded as a critical part of a communications network. The

function is also intrinsically linked to the protection of the encryption and integrity of user and control traffic.

Access and Mobility Management Function (AMF)

The handles the termination of the access network and user control plane, the connections of radio network base stations and terminal devices and their registration with the core network, and mobility management.

It plays a key role in network slicing and provides a terminal device access to all the slices provided to it. The AMF also establishes and manages connections outside the mobile network (non-3GPP access, e.g. WLAN). It also plays a role in the implementation of interception and monitoring of telecommunications (lawful interception or LI features).

This function controls and manages users' access to the network, which is why it must be regarded as a critical part of the communications network. The function is also essential for controlling network traffic, the maintenance of connections and ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

User Plane Function (UPF)

The UPF routes, directs and controls user traffic in the same way as SGW/PGW in 4G networks. It can be implemented in a decentralised and local manner, such as with edge computing (MEC)[26]. The UPF also controls the management of the quality of the user traffic service (QoS) and the maintenance of the continuity of sessions and services, which is essential for URLLC. The UPF also implements LI features.

This section also includes MB-UPF (Multicast/Broadcast User Plane Function), which processes and transmits parcels of group and general broadcasts to the radio part of the 5G network, and ensures traffic quality management (QoS).

This function controls and manages user traffic, which is why it must be regarded as a critical part of a communications network. The function is also essential for maintaining connections and ensuring the confidentiality of services and communications.

Policy Control Function (PCF)

The PCF is for traffic control and the implementation of the access management policy. The function utilises user traffic control parameters, from the UDR register, for example. The PCF plays a key role in controlling the quality and invoicing of network services. It includes support for network slicing, mobility policies and roaming.

This function controls and manages user traffic and access to the network, which is why it must be regarded as a critical part of a communications network. The function is also essential for the maintenance of connections and ensuring the availability of services.

[26] MEC in 5G networks. First edition – June 2018, ETSI White Paper No. 28, p. 8. https://www.etsi.org/images/files/ETSI-WhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf.

Authentication Server Function (AUSF)

The AUSF handles services and features linked to the authentication of users' terminal devices and provides a common authentication framework for both 3GPP and non-3GPP connections. The AUSF performs some of the same features as HSS in 4G.

This function controls and manages user traffic and access to the network, which is why it must be regarded as a critical part of a communications network. The function is also essential for ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Unified Data Management (UDM)

The UDM controls user identification, access management, subscription management, user registers and the creation and management of encryption keys. It maintains subscriber data management functions, such as the definition and deletion of 5G subscribers, the exchange of SIM cards, the changing of MSISDN numbers, and the modification and querying of order data. The UDM performs some of the same features as HSS in 4G. It also implements LI features.

This function controls and manages users' access to the network services, which is why it must be regarded as a critical part of a communications network. The function is also essential for controlling the communications network and its traffic, the maintenance of connections and ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Application Function (AF)

The AF supports routing decisions based on applications used by the users. It utilises the data defined for the NEF function and can interact with the core network via the NEF. The various network functions can perform the role of the AF. For example, the P-CSCF related to the implementation of IMS services can take over the role of the AF.

This function controls and manages network traffic and access to the network, which is why it must be regarded as a critical part of a communications network. The function is also essential for maintaining connections and ensuring the availability of services and the information security of the communications network as a whole.

Network Exposure Function (NEF) and Intermediate NEF (I-NEF)

The NEF enables the provision of the 5G core network features to third party operators and external applications. The NEF is used for promoting network services in, for example, 3GPP networks, the transmission of application data from outside the network to the mobile network and the internal controls of the gateway.

The NEF allows the AF to communicate safely with the network. It can also store information acquired from other functions in the UDR. The I-NEF acts as a NEF in roaming.

This function controls users' access to network functions, which is why it must be regarded as a critical part of a communications network. The function is also essential for maintaining connections and ensuring the availability

of services, the confidentiality of communications and the information security of the communications network as a whole.

Network Repository Function (NRF)

The NRF ensures the availability, registration and authorisation of network services. It maintains a list of network services and components, thus providing registration and search features and enabling the mutual availability and communication of other network functions and services. All of the 5G network functions interact with the NRF.

This function controls access to network resources and services by maintaining and communicating information about them, which is why it must be considered a critical part of a communications network. The function is also essential for ensuring the availability of services and the information security of the communications network as a whole.

Network Slice Selection Function (NSSF)

The NSSF manages network slicing services and specifications, and controls and controls AMF functions. The NSSF defines the AMF serving the terminal and terminates the network slices permitted got, and provided to, the terminal.

This function controls and manages traffic in the network and users' access to the network, which is why it must be considered a critical part of a communications network. The function is also related to the maintenance of connections and ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Network Slice Specific Authentication and Authorisation Function (NSSAAF)

The NSSAAF manages slice-specific authentication and authorisation together with the AAA server and the AAA proxy.

This function controls and manages users' access to the network, which is why it must be regarded as a critical part of a communications network. The function is also essential for ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Session Management Function (SMF)

The SMF combines the control traffic functions of session management. It controls session management according to the network protocols, the allocation of IP addresses and the directing of the UPF feature on a session-specific basis. The SMF also implements LI features.

This section also includes the Multicast/Broadcast Session Management Function (MB-SMF) function, enabling group and general broadcasts, and which manages sessions of MBS functions, controls quality (QoS) and configures MB-UPF for the transmission of traffic. The MB-SMF also allocates group and broadcast identifiers (TMGI) and coordinates, through the AMF, the use of resources in the radio network.

This function controls and manages network traffic, which is why it must be regarded as a critical part of a communications network. The function is also essential for maintaining connections and ensuring the availability of ser-

vices, the confidentiality of communications and the information security of the communications network as a whole.

Security Edge Protection Proxy (SEPP)

The SEPP is a proxy that supports concealment of the network topology and the filtering and monitoring of messages at control plane interfaces between mobile networks. It acts as a reliable access management function for other networks (e.g. IPX networks in the case of roaming).

This function controls and manages network traffic and access to the network, which is why it must be regarded as a critical part of a communications network. The function is also essential for maintaining connections and ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Unstructured Data Storage Function (UDSF)

The UDSF is an optional function that can be used by the other network functions to store and retrieve unstructured data. Such data may include information related to the function's connections, sessions or status, for example. The UDSF may be function-specific, or the functions may use a common shared UDSF.

This function controls and manages network traffic, which is why it must be regarded as a critical part of a communications network. The function is also essential for ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Unified Data Repository (UDR)

The UDR is a data repository that can store and retrieve subscriber data from UDM, data related to protocols from PCF, as well as structural and application data from NEFs. A network can have multiple UDR functions, and an UDR can serve either a single network function or a set of network functions. The UDR can also be integrated into a single network function.

This function controls and manages network traffic, which is why it must be regarded as a critical part of a communications network. The function is also essential for ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

UE Radio Capability Management Function (UCMF)

The UCMF records and stores terminal devices' ID-specific radio capability data specified by the communications network or by the terminal device manufacturer. The radio capability data includes supported radio technologies and frequency bands as well as other radio network capabilities. The UCMF communicates with the AMF by providing it with this information. The UCMF can also operate in a 4G network, where it communicates with the MME.

The data in UCMF is not sensitive in itself, but they control the operation of the network. A threat connected to the manipulation of the UCMF data is a downgrade attack, which may be limited by network implementation, however.

This function controls and manages access to the network, which is why it must be regarded as a critical part of a communications network. The function is also essential for ensuring the availability of services.

Non-3GPP InterWorking Function (N3IWF)

The N3IWF enables access to the 5G core network via a wireless local area network (WLAN). N3IWF supports the creation of an IPsec tunnel with a terminal device and authorises user access to the 5G core network. The IPsec tunnel and the N2 and N3 interfaces, i.e. the user and control plane, are terminated in N3IWF.

This function controls and manages network traffic and access to the network, which is why it must be regarded as a critical part of a communications network. The function is also essential for maintaining connections and ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Trusted Non-3GPP Gateway Function (TNGF)

The TNGF acts as a gateway between terminals and the 5G network when a trusted non-3GPP Access Network (TNAN) is used as an access network.

The TNGF is used for the identification of terminal equipment and access to the network when the terminal equipment is registered via the TNAN network. In addition, the functionality contributes to network control functions, such as mobility management and the allocation of connection resources within its area.

TNGF terminates the N2 and N3 interfaces, i.e. the processing of user and control traffic takes place through it. The function controls and manages traffic in the network and access to the network, which is why it must be regarded as a critical part of a communications network in order to enable safe and controlled access to a 5G network via reliable, non-3GPP based networks.

Trusted WLAN Interworking Function (TWIF)

The TWIF enables devices that are not capable of 5G signalling (Non-3GPP 5G Capable WLAN devices) to access the 5G core network via a wireless local area network (WLAN).

It handles both control and user-level traffic and serves as a gateway between the WLAN and the 5G core network, and terminates N1, N2 and N3 interfaces. In addition, it carries out the selection procedure for the AMF and handles the control traffic in the 5G network.

This function controls and manages network traffic and access to the network, which is why it must be regarded as a critical part of a communications network.

Wireline Access Gateway Function (W-AGF)

The W-AGF acts as a gateway between terminal devices, in this case 5G-RG (5G Residential Gateway, 5G-RG) or FN-RG (Fixed Network Residential Gateway, FN-RG), and the 5G network when the access network used is a fixed network. The W-AGF terminates N2 and N3 interfaces, i.e. the processing of user and control traffic takes place through it. It also implements the registration of the terminal device (in the case of the FN-RG).

This function controls and manages network traffic and access to the network, which is why it must be regarded as a critical part of a communications network.

Short Message Service Function (SMSF)

The SMSF transmits SMS messages between the 5G core network and the SMSC. This functionality checks the SMS service information related to the user's subscription and ensures that the messages are sent accordingly in the N1 interface.

The SMSF is also involved in the billing of SMS messages and also plays a role in the implementation of interception and monitoring of telecommunications (lawful interception or LI features).

This function controls and manages user text message traffic, which is why it must be regarded as a critical part of a communications network.

5G-Equipment Identity Register (5G-EIR)

The 5G-EIR is a mobile network database that stores International Mobile Equipment Identities (IMEIs) and contains information on the authorisation of the use of mobile devices. Normal use of terminal devices included in the 5G-EIR blacklist in a communications network is not allowed.

This function controls and manages users' access to the network, which is why it must be regarded as a critical part of a communications network. The function is also essential for ensuring the availability of services.

Service Communication Proxy (SCP)

The SCP plays an important role in a 5G network, transmitting and re-routing messages to other network functions. The SCP manages, for example, the simplification of topology, load balancing and sharing, the processing of overload and the harmonisation of message parameters to facilitate integration in multi-supplier environments.

This function controls and manages network traffic, which is why it must be regarded as a critical part of a communications network. The function is also essential for maintaining connections and ensuring the availability of services, the confidentiality of communications and the information security of the communications network as a whole.

Network Data Analytics Function (NWDAF)

The NWDAF is for the collection, analysis and dissemination of data from the 5G network functions, maintenance and management system (OAM) and terminal devices. This function supports the use of machine learning models, as well as their training and distribution [to other possible NWDAF functions if the network implementation includes several NWDAF functions].

The NWDAF provides both real-time and retroactive analysed data to the network functions. In addition, the NWDAF produces a predictive analysis to support proactive management of the 5G network. The data collected by the NWDAF can be used for automated network infrastructure scaling, the selection of network slices, roaming analytics, or the management of access and mobility, for example. The system also includes the functionalities of the DCCF and ADRF function, where they are not implemented as separate network functions, but as part of the NWDAF.

The NWDAF function controls and manages traffic in the network, an essential function, which is why it must be considered a critical part of a communications network. The function is also essential for ensuring the availability of services.

Data Collection Coordination Function (DCCF)

The DCCF centrally produces information to guide the operation of the 5G network. It manages and maintains orders for network functions, and transmits data to subscriber functions and terminal devices.

The DCCF also formulates and processes the data it collects. In this way, it is possible to determine, for example, the time window used to transmit information, relationships with other network events (data), or the extent to which data are collected before sending them to a subscriber.

The DCCF also performs the function of collecting and transmitting the data to be analysed, for example to network functions and network control and maintenance functions. Analytics may also be stored as statistics or predictive models in the NWDAF function. In this case, access to the stored analytics is possible by means of the DCCF. Additionally, the function instructs the Messaging Framework (MF) through the Messaging Framework Adapter Function (MFAF) functionality, in connection with the sending, formatting and processing of data.

Analytics Data Repository Function (ADRF)

The ADRF is a data warehouse that stores, retrieves and manages data, analytics, and machine learning models for the use of other 5G network elements (and network management).

The ADRF provides an interface through which other 5G network functionalities, such as the NWDAF, can store or retrieve information, analytics and machine learning models. In addition, on the basis of its specifications or a request, the DCCF (Data Collection Coordination Function) may direct the storage of data to the ADRF, either directly or indirectly. The other 5G network functions may also request the DCCF to store the analytics received from the source in the ADRF.

The ADRF can also manage machine learning models. This entails the storage, making available and removal of models. In such a case, the ADRF must check whether the network function that made the service request has the authority to use the data, and, if so, the ADRF will provide the requested data, analytics or machine learning models to the function in question.

The function essentially controls and manages traffic in the network, by storing and producing information that has a key impact on the operation of the network, which is why it must be regarded as a critical part of a communications network.

Network slice Admission Control Function (NSACF)

The NSACF is a function associated with 5G network slicing, which controls and limits the number of terminal devices and PDU connections in each network slice. This function prevents overload and ensures the controlled use of slice resources. If the maximum quantity per slice is reached, the NSACF may

reject the request. In this case, the user may be given a back-off timer before a new attempt is permitted. The NSACF may also provide status information to other network functions and operate in conjunction with other functions that control slicing.

The function can be defined differently depending on the architecture of the network; one common NSACF across the network or several NSACF functions with their own service area or a hierarchical solution where one NSACF controls other, region-specific NSACFs.

This function controls and manages users' access to the network, which is why it must be regarded as a critical part of a communications network.

Time Sensitive Communication and Time Synchronization Function (TSSF)

The TSSF is a time synchronisation and time-critical communication function, providing highly time-critical and high-reliability communication services (Ultra Reliable Low Level Communications, URLLC).

The TSCTSF manages time synchronisation by connecting time synchronization requests for communications network functions to sessions, and monitors, distributes, and reports the state of network time synchronisation. The function maintains the time synchronisation status information for the communications network by collecting information from the radio network, the Network-side TSN Translator (UPF) or directly from other network components that generate synchronisation information. In addition, it acts as an instantaneous interpreter between the functions of the IETF network that is predictable and controlled in terms of delay and the functions of the 5G network.

The functionality will enable time-critical and high-reliability communication services by collecting, maintaining and sharing situational information related to time synchronisation and must therefore be considered as a critical part of the communications network.

6.4 International comparison of critical parts of the 5G network

In the EU common 5G risk assessment, the sensitivity of different parts of the radio network was thought to be quite high[27]. The sensitivity of the radio network was already considered high when the 5G risk assessment was being drawn up in 2019, even though the 5G network generation was only in the first phase of roll-out across the EU. In several EU Member States, the criticality of the 5G network is explicitly addressed in the context of the EU's common 5G risk assessment and toolbox. The suitability of the measures implemented on the basis of the common toolbox for a 5G radio network corresponds to the current or future situation in at least 17 Member States out of the 21 Member States where the measures were put in place with reference to the toolbox SM03[28]. These risk assessments and the toolbox are naturally supplemented by a function-based definition of the various parts and functions of the network relying on 3GPP specifications. A function-based definition of the various parts and functions of the network has also been selected

[27]NIS Cooperation Group, Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29 November 2020, CG Publication 01/2020Chapter 2.21, p 16-17 and Chapter 2.25, p 18.
[28] NIS Cooperation Group, Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity, June 2023, p 6-8.

in the countries known to Traficom where attempts have been made to specify technically the scope of the parts of 5G networks deemed critical, i.e. France and the United Kingdom.

At EU level, the definition of the criticality of networks is informed in particular by the strategic and technical measures in the EU's common 5G toolbox. For example, more than half of the EU Member States have imposed restrictions on high-risk equipment manufacturers as regards core network, network management and radio network functions. These parts of the network have thus been identified as critical in a large number of EU Member States and, if deemed nationally appropriate, communications network equipment may be removed from these parts of the network.

7 IP-based telephone services in a mobile network

This section supplements the other sections of the regulation. Under to this section, the critical elements of a communications network include the communications network functions and procedures included in an IP Multimedia Core Network Subsystem (IMS) according to the 3GPP technical specification 23.228 that are used to realise an IP-based public telephone service.

This section defines (IMS) Core as a critical part of a communications network in so far as it is used to realise an IP-based public telephone service.[29] General voice services are realised in IP-based 4G and 5G mobile networks solely with an IMS. It is also used to realise other multimedia services in IP-based mobile networks. The IMS Core functions are connected via interfaces to the 4G or 5G network, and they may be considered part of the network core.

According to section 3(42) of the SVPL, a public telephone service ,means a communication service used to make and receive national and international calls using a number in a national or international numbering plan.

With reference to this section, critical IMS Core features could include the Call Session Control Function (CSCF), Subscription Locator Function (SLF), Breakout Gateway Control Function (BGCF) and Media Gateway Control Function (MGCF).

Telephone services provided in mobile networks that are based on an IMS Core are in at least the VoLTE and VoWifi 4G network and the VoNR 5G network. This section does not require specifically the use of the 4G or 5G radio network in a telephone service; instead, the terminal device can also use WiFi, for instance, provided that it is a public telephone service provided by a telecommunications company.

Other voice services that are not based on IMS Core functions can also be realised via IP-based mobile networks. This section of the regulation does not include any provisions on such other services, and the potential criticality of functions related to them should be assessed on other grounds, as necessary.

8 Entry into force and transition period

The regulation will enter into force on x x 202x and will remain in force indefinitely. The regulation must enter into force one year after its adoption. This transition period is necessary in order to allow, in particular, smaller telecom-

[29] IMS Core Reference Architecture, 3GPP TS 23.228.

munications operators sufficient time to prepare for the entry into force of the updated regulation.

This also takes into account the comment in the Advisory Board on Network Security's recommendation of 16 June 2025 on the Regulation of the critical parts of communications networks, according to which the Advisory Board considers it important that the assessment of the criticality of communications networks takes into consideration the predictability and legal certainty of investments in communications networks and the international standards on which the construction of communications networks is based. In the updating work, it is recommended to assess the need for possible transition periods, while at the same time considering the lifecycles and the objectives of the regulation.[30]

In addition, the Advisory Board's recommendation includes the notion that the assessment should focus attention on EU policies and recommendations, as well as general international developments. The recommendation refers to the Commission's 2023 Communication on the Security of 5G networks[31]. In the Communication, the Commission urges the Member States, when implementing the measures in the 5G toolbox also to focus attention as closely as possible on the recommendations presented in the progress report, in particular with regard to the use of transition periods,[32] for example[33].

As regards the objectives of the rules underlying the power to issue regulations, it is important to note that it implements a measure in the European Union's common toolbox for the security of 5G networks concerning the protection of critical parts of the network. The preliminary work for the Act stresses that the supervisory authority must be able to prohibit the use of equipment in a public communications network if functions that are of critical importance for society would be jeopardised if the availability, confidentiality and integrity of information are compromised in the communications network[34]. The progress report recommends attention being paid to the risk associated with the use of transition periods[35].

With the entry into force of the new regulation, the Regulation of the Finnish Transport and Communications Agency of 19 May 2021 on critical parts of the communications network (TRAFICOM/161584/03.04.05.00/2020) is repealed.

[30] Recommendation of the Advisory Board for Network Security regarding the Regulation on the critical parts of communications networks, 16 June 2025, VN/15573/2022.
[31] Communication from the Commission – Implementation of the 5G Cybersecurity Toolbox, 15.6.2023, C(2023) 4049 final.
[32] NIS Cooperation Group, Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29.11.2020, CG Publication 01/2020. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[33] NIS Cooperation Group, Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity, June 2023, s 23.
[34] Government proposal HE 98/2020, p 261:
[35] NIS Cooperation Group, Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity, June 2023, p 23.

Monitoring

The Finnish Transport and Communications Agency will regularly assess the need to update the regulation. The assessment work will take account of any future recommendations of the Advisory Board for Network Security, the development of communications network technology and network -and network implementations

References

Finnish governmental sources

HE 98/2020. Government proposal to Parliament for an Act amending the Act on Electronic Communications Services and for certain related acts

Report of the Transport and Communications Committee LiVM 16/2020 – HE 98/2020

Statement by the Constitutional Law Committee PeVL 35/2020 – HE 98/2020p

Report on 5G: Cybersecurity. Abstract. Finnish Transport and Communications Agency. Traficom Publications 14.5.2019. https://www.traficom.fi/fi/ajankohtaista/liikenne-ja-viestintavirasto-julkaisi-selvityksen-5gn-kyberturvallisuudesta

Recommendation of the Advisory Board for Network Security on the Regulation on the critical parts of communications networks, 16 June 2025, VN/15573/2022.

Publications of the European Union

Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures. CG Publication 01/2020. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

ENISA Threat Landscape for 5G Networks. Updated threat assessment for the fifth generation of mobile telecommunications networks (5G). 14.12.2020. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

EU coordinated risk assessment of the cybersecurity of 5G networks. Report. 9 October 2019. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049

Foreign governmental sources

NCSC advice on the use of equipment from high-risk vendors in UK telecoms networks. 28.1.2020, updated on 14 7 2020. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

Other

3GPP TR 33.848 V0.5.0 (2019-11). Study on Security Impacts of Virtualisation. https://www.3gpp.org/DynaReport/33848.htm

3GPP TS 21.905. Vocabulary for 3GPP Specifications. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=558

3GPP TS 23.002. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network architecture (Release 16)

3GPP TS 23.228. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 16)

3GPP TS 23.273. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional stage 2 description of Location Services (LCS) (Release 16)

3GPP TS 23.273. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 5G System (5GS) Location Services (LCS); Stage 2 (Release 16)

3GPP TS 23.501. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects System architecture for the 5G System (5GS); Stage 2 (Release 16)

3GPP TS 32.240. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging architecture and principles (Release 16)

3GPP TS 36.300. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 15)

3GPP TS 38.300. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description; Stage 2 (Release 15)

ETSI: MEC in 5G networks. First edition – June 2018, ETSI White Paper No. 28. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf