Report on the cybersecurity of Open RAN

11 May 2022

NIS COOPERATION GROUP

Table of content

1. Introduction

Policy context

1.1. The timely deployment of secure 5G networks is a high priority for the European Union (EU). To contribute to this objective, EU Member States, with the support of the European Commission and the EU Agency for Cybersecurity (ENISA), have developed a concerted approach to the cybersecurity of 5G networks. Through this concerted approach, EU Member States jointly assessed the main risks related to 5G networks ('EU Coordinated risk assessment')[1] and on this basis, identified a set of common risk mitigating measures presented in the form of an EU Toolbox[2] in January 2020.

1.2. Among other risks, the EU Toolbox has highlighted that significant risks can originate from the supply chain of 5G networks. As a follow-up to the publication of the EU Toolbox, Member States authorities have stressed the importance to monitor security issues related to new trends and developments in the 5G supply chain.

1.3. 5G networks offer new mobile network functions and use new networking technologies, in the mobile core network, transport network and radio access network (RAN). In the EU Coordinated risk assessment, the core network functions were rated as critical, and RAN functions as highly sensitive. Compared to 4G, 5G introduces new functions such as edge computing and low latency communications. 5G also potentially changes how network functions are delivered, by using cloud computing, network function virtualisation, and intelligent network functions based on machine learning. Generally speaking, these new technologies allow operators to manage the network better and have more flexibility and scalability, both in the core and in the access network. In Open Radio Access Networks (Open RAN), some of these new technologies, such as cloudification and virtualisation[3], are used to allow for more interoperability between different network components in the RAN (more details in Box 1).

1.4. Since the EU Toolbox was adopted, the topic of Open RAN has received significant attention and interest. Today, mobile network operators (MNOs) source their entire RAN from one supplier or use multiple suppliers in different geographic areas. One of the key characteristics of Open RAN is to allow that RAN components from different suppliers are interoperable and so, when deployed in the same geographic area, they can work together. In order for network elements from different suppliers to be interoperable, they need to have open interfaces, i.e. their interfaces need to follow open standards. Hence, the development of open interfaces, but not necessarily currently of open standards[4], lies at the heart of the Open RAN paradigm. Other enablers for Open RAN are the splitting/disaggregating of different network functions, and the cloudification and virtualisation of network functions.

1.5. By facilitating the use of different suppliers in the RAN, Open RAN could in the medium to long term contribute to the implementation of strategic measure 05 of the EU Toolbox, which recommends

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

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

[3] Virtualisation creates an abstraction layer on top of the hardware, a so-called hypervisor, for software to run on. Cloudification means that the software is no longer running locally, but in a central cloud infrastructure, https://www.redhat.com/en/topics/cloud-computing/cloud-vs-virtualization

[4] While considering point 3.5. 'Supporting Action 03' of this report and point 4.9 on addressing deficiencies in the development of technical specifications.

ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies, in order to avoid or limit any major dependency on a single supplier.

1.6. In this context, Member States have decided that an in-depth analysis of the security implications of Open RAN is needed, looking at both security opportunities and risks, as this concept is in early stages of development and technical specifications are being developed. The aim of the analysis is to identify whether further recommendations and/or actions are required as regards the deployment of Open RAN networks.

Scope and objectives

1.7. This report focuses on security aspects considered particularly important from an EU perspective. This includes aspects related to EU capacities and strategic autonomy to the extent that they contribute to the EU's security objectives.

Box 1: What is Open RAN?

The RAN is the link between terminal equipment and the core network in a telecommunications mobile network[5]. The established RAN architecture is fully integrated, sourced from a single supplier as a proprietary integrated hardware and software solution. Today, the hardware used in the RAN is explicitly built for the supplier and is not able to host software from other suppliers. Open RAN is a new paradigm for building the RAN, which aims to allow telecom operators to use hardware and software solutions from several different suppliers, even within the same geographic area.

The key characteristics of Open RAN architectures are:

1. **Open interfaces[6]**: Splitting the radio functions of the RAN and defining interfaces on top of the 3rd Generation Partnership Project (3GPP) ones between different RAN components;
2. **Cloudification**: Cloudification, softwarisation and virtualisation of the network functions in the RAN separating the software from the hardware (i.e. disaggregation) and moving from specifically-design hardware to general-purpose hardware;
3. **Automation**: RIC (RAN Intelligent Controller) for RAN orchestration and management opening the door to advanced Machine Learning (ML)/Artificial Intelligence (AI) functionalities.

The softwarisation, cloudification and virtualisation (and therefore the disaggregation) of the network functions in the RAN, as well as the application of ML and AI are cross-cutting trends in 5G networks, not specific to the Open RAN paradigm. The introduction of open interfaces, which is specific to Open RAN, is one of the factors allowing vendor diversification. While also touching upon

[5] In addition, the transport network provides connectivity between the RAN and the core network.

[6] The term 'open interface' is used to abbreviate 'an interface using open standards'. These open standards can be used by other suppliers to make interoperable products. With a proprietary or 'closed' interface, it is not always possible for another supplier to make products that are interoperable. The term 'open' does not mean that the interface is unguarded, insecure or unprotected. A proprietary interface, also called 'closed' interface, is not necessarily more guarded or more secure. In addition, Open RAN can also use open source software, where the source code is publicly available for anyone to inspect, modify or enhance. Similarly, the publicly available interface definitions would be available for anyone to inspect, modify or enhance, and to develop tools to evaluate security of implementations.

cloudification and automation, this report will mostly focus on the open interfaces introduced by Open RAN.

Open RAN is a network architecture paradigm, not a specific standard nor a single approach. There are several Open RAN concepts, ideas and initiatives, and several technical specifications, developed and advocated by several different groups, each taking a slightly different approach and using different specifications including virtualised RAN (v-RAN) and O-RAN[7].

Open RAN stakeholders

1.8. The main stakeholders in the 5G ecosystem are:

- MNOs: entities providing mobile network services to users, operating their own network with the help of third parties[8].
- Suppliers of mobile network operators: entities providing services or infrastructure to MNOs in order to build and/or operate their networks. This category includes:
    - Network equipment manufacturers;
    - Other third-party suppliers, such as cloud service and infrastructure providers, systems integrators, compute and storage hardware suppliers, suppliers of network software functions, security and maintenance contractors, transmission equipment manufacturer.
- Manufacturers of connected devices: entities providing objects or services that will connect to the 5G networks (e.g. smartphones, connected vehicles, e-health).
- Other stakeholders: including service and content providers, end-users of 5G mobile networks, and government services that have legal interception and tapping authority.

1.9. In Open RAN architectures, some of these stakeholders would have a more prominent role, such as systems integrators and cloud service/infrastructure providers.

Standardisation and technical specifications

1.10. 3GPP, a partnership bringing together Standard Development Organisations (SDOs) from different continents, is the main global body for developing standards for mobile communications. It is a collaboration between seven Organisational Partners, from Europe (ETSI), USA (ATIS), China (CCSA), Japan (ARIB, TTC), Korea (TTA) and India (TSDSI). 3GPP technical specification groups have standardised industry security features in 3G, 4G and 5G standards. 3GPP develops global specifications for complete cellular networks from all generations, from 2G to 5G. 3GPP is working on specifications for RAN interfaces, as well as specifications for the Open RAN network architectures.

1.11. In addition, a number of industry-led bodies[9] develop technical specifications for Open RAN architectures, in particular the O-RAN Alliance. The O-RAN Alliance was founded in August 2018 by

[7] Open RAN aims to build RAN solutions on general-purpose vendor-neutral hardware, open interfaces and software. In v-RAN, the processing functions are partially virtualised and run on top of standardised servers. In O-RAN, the RAN functions are split and virtualised with standard interfaces. This report focuses on the general paradigm of Open RAN, rather than on the individual specifications and industry groups.

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

[9] Other industry-led bodies such as the Telecom Infra Project (TIP) also play a role in in promoting, training and implementing Open RAN solutions worldwide. TIP was launched in 2016 to accelerate the development and deployment of open, disaggregated and standards-based technology solutions.

five telecom companies[10]. The Alliance works on specifications covering three different areas: RAN disaggregation, RAN automation and RAN virtualisation. The O-RAN Alliance specifications complement the 3GPP ones by defining new requirements and use cases, interface profiles, additional new open interfaces and new components.

Deployment of Open RAN - Market aspects

1.12. The future impact of Open RAN on the market for network equipment is not fully clear at this stage. According to a survey of MNOs operating in the EU carried out by the Body of European Regulators for Electronic Communications (BEREC)[11], Open RAN is not yet deployed at a significant level in the operations of commercial networks, but will become a commercial reality in the near or medium-term future. The survey showed that the implementation of Open RAN in its different aspects will take some time due to its lack of maturity, and ensuring interoperability is essential for its successful implementation.

1.13. Based on a study on 5G supply market trends[12], it can be expected that most large-scale 5G deployments will rely on established approaches to the RAN architecture, rather than an Open RAN approach. MNOs who have already bought 5G RAN equipment may consider a hypothetical switch in the mid to long term, as the lifetime of RAN equipment is usually about a decade. As of today, only a limited number of Open RAN deployments exist across the world, with only one extensive commercial network based on Open RAN in Japan.

Methodology

1.14. This report is based on the results of a security analysis performed by Member States, with support from the Commission and ENISA. It brings together the results from the following activities carried out in the course of 2021 and early 2022:

- An in-depth security analysis by Member States looking at a) the impact of Open RAN on security risks of 5G networks already identified in the EU Coordinated risk assessment of 5G cybersecurity of October 2019, and b) identifying and assessing potential new security risks and potential security opportunities related to Open RAN;
- Workshops and information exchange within the NIS Work Stream on 5G Cybersecurity;
- A comprehensive review of publicly available information sources on technical security aspects of Open RAN, conducted by ENISA (this included 67 information sources such as reports and research notes from industry, advocacy, academia and public authorities);
- An analysis of the O-RAN Alliance specification development process, conducted by ENISA for the NIS Sub-group on 5G standardisation and certification;
- A survey addressed to MNOs on Open RAN market aspects, conducted by BEREC.

1.15. Open RAN is a relatively new and rapidly evolving concept. Open RAN usage scenarios and technical specifications are still uncertain and not fully determined yet, in particular when it comes to security. The findings presented in this report are reflecting only the current situation and highlighting only

[10] The O-RAN Alliance defines three areas of activity, namely: "Specification development"; "Development of open software for the RAN"; and "Support O-RAN Alliance member companies in their efforts of testing and integration of their O-RAN implementations", https://www.o-ran.org/about

[11] An overview of the BEREC work on the Open Radio Access Network (RAN), BoR (22) 23, 10 March 2022, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/10204-an-overview-of-the-berec-work-on-the-open-radio-access-network-ran – The survey gathered answers from 73 MNOs operating within the EU.

[12] 5G Supply Market Trends, 10 August 2021, https://op.europa.eu/en/publication-detail/-/publication/074df4ff-f988-11eb-b520-01aa75ed71a1

some of the most salient issues relevant for the security of 5G networks. The risks identified in this report may change with future evolutions of the Open RAN specifications and technology and will depend on the way in which Open RAN is deployed by MNOs.

2. Security assessment of Open RAN

2.1. Overall, the NIS Cooperation Group concludes that Open RAN will have a significant impact on a number of risks that were already identified in the EU Coordinated risk assessment of 5G networks published in October 2019. In addition, it identifies several new risks and vulnerabilities introduced by Open RAN. If not adequately mitigated, those risks could have a particularly strong negative impact on the security of large-scale 5G deployments using Open RAN. Annex 1 gives an overview of all risks identified and analysed in this report. The report identifies as well potential opportunities that stem from using Open RAN solutions, an overview of which is presented in Annex 2.

Impact of Open RAN on identified security risks (EU Coordinated risk assessment, October 2019)

2.2. In the EU Coordinated risk assessment of 5G networks from 2019, the NIS Cooperation Group identified a number of categories of risks with nine concrete risks of strategic importance from an EU perspective. These risks remain relevant, to various extents, to Open RAN deployments, and can evolve (i.e. be reduced or amplified) in Open RAN networks.

Risks amplified in Open RAN networks compared to established networks:

- Misconfiguration of networks: Integrating more components from different suppliers, the use of virtualisation management and the lack of mature MNO processes for complete lifecycle of Open RAN deployment greatly increase configuration complexity and the risk of misconfiguration of networks and render faults more likely. Moreover, the lack of mature standards can lead to dissimilar and potentially poorer network design and architecture which increases the risk for ineffective emergency and continuity mechanisms. Due to the complexity and many possible combinations of software and hardware, or combinations of software components, integrating the security features may require additional effort and could lead to an increased risk that security features are not used.

- Low product quality: Open RAN means an increased number of components from different suppliers present in the RAN, which increases the risk of diverse levels of security among those components. It is unclear whether newcomers in the Open RAN market might prioritise innovation or security in the short-term, and considering that these different components will be interconnected, there is an increased risk that one vulnerable component (the weakest link) jeopardizes the security of the overall network.

Risks moderately amplified or similar in Open RAN networks compared to established networks:

- Lack of access controls: The increased number of suppliers involved in the network could mean having to grant access to more parties during its operation, for example, to remedy a malfunction. MNOs may also choose to outsource more operations to third parties (e.g. system integrators) given the increased network complexity.

- State interference through the 5G supply chain*:* More suppliers available in the network could lead to exposure to a higher number of supply chain risks. The risk profile of individual suppliers, which can be assessed based on the criteria recommended in the EU Coordinated risk assessment[13], continues to be an important source of vulnerabilities.

[13] See point 2.37 of the EU Coordinated risk assessment.

- Exploitation of 5G networks by organised crime*:* The increased number of interfaces and suppliers could offer more opportunities for organised crime groups (OCGs) to enter and disrupt the network.

- Significant disruption of critical infrastructures or services: A number of identified risks, in particular linked to the increased number of suppliers, new open interfaces and the lack of fully mature Open RAN and network function virtualisation (NFV) security controls mean that critical national infrastructures relying on 5G networks could also be more exposed to incidents.

- Massive failure of networks due to an interruption of electricity supply or other support systems: Whether it is an established or an Open RAN architecture, adequate power supply (including backup) needs to be in place.

- Internet of Things (IoT) exploitation: Open RAN components, the network functions running on them, but also for example virtualised Multi-Access Edge Computing (MEC) applications, would be vulnerable to attacks from connected terminals, such as IoT devices, but the risk would be similar for network components in an established RAN architecture.

Risk reduced in Open RAN networks compared to established networks[14]:

- Dependency: The potential to enable the emergence and use of more suppliers in the RAN coupled with a disaggregated RAN, interoperable interfaces and increased use of commercial off-the-shelf (COTS) hardware and possibly open source software, could help reduce the risks related to dependency on a single supplier.

New security risks of Open RAN

2.3. New security risks related to Open RAN networks and not covered by the EU Coordinated risk assessment of 5G networks have also been identified. More details and examples of risk scenarios can be found in Annex 1.

- Expanded threat surface and vulnerabilities in Open RAN functions and interfaces: The threat surface expands due to an increased number of suppliers, components and interfaces forming part of Open RAN deployments. For example, fronthaul interfaces could be exploited to carry out denial-of-service attacks, interception or tampering attacks and, as a result, compromise availability, confidentiality and/or integrity. In addition, by opening certain interfaces, Open RAN will give access to information flows to new third-party applications, which raises security issues with regard to data passing through the network (e.g. real-time location data of users connected to the network).

- Open RAN network fault management complexity: In a multi-vendor setup, the complexity of identifying and resolving a network malfunction is likely to increase, also expanding the amount of time necessary to identify and resolve it. In addition, in some cases, several different suppliers may be required to provide remote support, further increasing the risk. Moreover, more Open RAN suppliers could mean that it is harder to allocate and enforce liability to one or more suppliers.

[14] See also section on Security opportunities (point 2.6. 'Supplier diversity in the RAN').

- Deficiencies in the O-RAN technical specifications development process: Security has not featured at the forefront of the technical specifications development process of the O-RAN Alliance[15]. Immature O-RAN specifications without security taken into account from the start may lead to gaps in the specifications and insecure RAN products. In addition, key decision rights within the O-RAN Alliance are conferred to the Board, which is composed only of a subset of the members and only of MNOs. The stringent provisions of the O-RAN Alliance Adopter License Agreement might hamper the transfer of information and knowledge between adopters and non-adopters, making discussions outside the O-RAN Alliance more difficult.

- New or increased dependency on cloud service/infrastructure providers: Virtualisation and the use of cloud is becoming more widespread in the telecoms sector, in particular in Open RAN deployments. There is a risk of MNOs becoming dependent on a small number of cloud service/infrastructure providers, which could lead to supplier lock-in. In addition, if networks rely on the same cloud provider, this could exacerbate vulnerabilities[16].

- Decreased sustainability of the EU 5G supply chain and potential dependencies on non-EU capacities: The RAN supply market could be transformed in a way that gives momentum to new players (e.g. system integrators, cloud service/infrastructure providers, etc.), including large non-EU players. This could lead to new critical dependencies in the mid- to long-term, or increase existing ones[17], with potentially significant impacts on security.

- Impact of Open RAN mix and match approach on network security and performance: The integration of components from multiple suppliers may not always be seamless. For example, it may create security vulnerabilities and lead to decreased performance due to the number of different network elements, interfaces and resource-demanding protection mechanisms. In addition, different releases of the same software might be deployed in a heterogeneous way.

- New risks due to resource sharing: In Open RAN, different network functions are virtualised and running on the same hardware, which means that potentially, if there are not sufficient controls in place, other network functions could be impacted by security issues with these new RAN functions.

2.4. In addition, it should be noted that the virtualisation of network functions, a general trend in the evolution of network equipment and a key feature of Open RAN, can introduce new risks such as misconfiguration of the virtualised network functions and software vulnerabilities for example in the hypervisor, or in service management and orchestration functions[18].

[15] Open RAN Risk Analysis, commissioned by the German Federal Office for Information Security (BSI), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5GRAN-Risk-Analysis.pdf?__blob=publicationFile&v=7

[16] This risk is also applicable in 5G core networks, if core network services are deployed in public cloud environments or deployed as services in the future.

[17] High technology dependence has been identified in a number of areas, such as on components and cloud (Strategic dependencies and capacities, 5 May 2021, SWD(2021) 352 final).

[18] ENISA Network Function Virtualisation Security in 5G, Challenges and Best Practices, 24 February 2022, https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

Security opportunities of Open RAN

2.5. Open RAN could also bring a number of security opportunities. However, their realisation is conditional upon a number of factors set out below and will vary depending on the evolution of the Open RAN specifications and the uptake of Open RAN in the market. Moreover, some counter-risks are associated with those potential opportunities. Therefore, the assessment related to security opportunities remains more speculative than the one related to security risks.

2.6. For example, for many of these opportunities to really materialise, open interfaces need to be mature, robust and highly standardised. Their specifications need to be developed in accordance to the requirements for standardisation organisations (including openness and transparency). Moreover, standards need to be accepted by the ecosystem (industry and national authorities). Deploying Open RAN also supposes that MNOs as well as national competent authorities who will perform audits have sufficient resources and technical expertise to deal with a more complex architecture. The potential use of open source in Open RAN may also require a certain level of visibility of software sourcing and codes to enable examination (manually or by tools). Annex 2 presents in more details the various security opportunities, their enabling factors and caveats. Some of those opportunities are increased by Open RAN and some are present in but not specific to Open RAN.

Security opportunities increased by Open RAN:

- Supplier diversity in the RAN: The potential of Open RAN to enable the emergence and use of more suppliers in the RAN coupled with a disaggregated RAN, interoperable interfaces and an increased use of open source and commercial off-the-shelf (COTS) hardware could help reduce the risks related to dependency on a single supplier. However, the market could also reconsolidate around a small number of suppliers, system integrators and cloud service/infrastructure providers, thus negating the diversification opportunity. New entrants might prioritize time to market or adopt a free-rider attitude, reducing incentives to invest in security. Furthermore, dependencies deeper in the supply chain of critical components (e.g. chips) may still exist.

- Interoperability: A higher number of components with open interfaces increases interoperability in the RAN. Open RAN could also bring more flexibility and dynamic networks, with the ability to swap subcomponents out as required without the need to replace the entire RAN. System integrators will have a central role to ensure smooth integration and interoperability. On the other hand, the increased number of suppliers also bring challenges for interoperability testing, maintenance of releases as well as liability issues, causing potential delays, for example in network repair measures.

- Visibility and auditing: The use of open standards[19] for the interfaces between RAN components means that different RAN components from different suppliers connect with each other in a similar way, which could improve visibility and transparency. As regards auditing, the use of open standard interfaces could make it easier for auditors and security testers to understand how a certain RAN implementation is working and if it is working correctly. The increased use of open source in Open RAN could similarly allow for greater visibility and transparency about how components work on the inside. However, it should be noted that open source is not a guarantee for better security, and it is well-known that vulnerabilities may exist in both closed and open source software.

[19] While considering point 3.5. 'Supporting Action 03' and point 4.9 on addressing deficiencies in the development of technical specifications.

- Role of EU-based suppliers: Open RAN could bring some opportunities for EU-based suppliers, including small and medium-sized enterprises (SMEs) and start-ups, to specialise in some areas and play a role in the Open RAN market. Already established EU suppliers could be well placed to take on the role of system integrators. However, as noted above in section 2.3, non-EU players are also strongly positioned to play a role in this market as either suppliers, notably on the software level, or system integrators. This could lead to new or increased dependencies in the mid-to long-term. Therefore, the presence of EU players could benefit from being strengthened through investment and support for research and development (R&D), while respecting competition rules.

Security opportunities present in but not specific to Open RAN:

- Automation: The introduced intelligence in Open RAN can be used to automate the management and control via big data analysis, AI and ML. As a consequence, closed loop responses to changes in the network can be automatically performed. This has the potential advantage that the need for human interactions may be reduced, which may decrease threats related to human error. At the same time, automation can also bring additional security, liability and availability risks, and MNOs could lose control over critical processes.

- Cloudification and virtualisation: While being a general trend in the evolution of network equipment, virtualisation and cloudification are key features in the Open RAN architecture. Virtualisation and cloud-based solutions allow for greater flexibility and make managing network resources easier. Nevertheless, virtualisation and cloud could also bring some risks related to, inter alia, implementing and operating virtualisation and containerisation (e.g. handling hypervisor-related vulnerabilities); secure orchestration and management; a need for effective and secure administration and access controls; and incorporating new and legacy technologies.

3. Guidance on Toolbox implementation for Open RAN deployments

3.1. To achieve a timely and secure deployment of 5G networks, the implementation of the EU Toolbox is essential and forms an important baseline for securely deploying 5G networks using Open RAN. As explained in the previous chapters, Open RAN has the potential to increase diversification of suppliers and interoperability in the RAN. However, Open RAN can also exacerbate a number of risks of 5G networks and bring new risks that need to be managed.

3.2. Therefore, while all the EU Toolbox measures remain relevant, some are particularly important in Open RAN deployments, and in some cases may require adjustments in their actual implementation to mitigate the risks associated with Open RAN networks. The set of mitigating measures presented below builds upon the EU Toolbox measures and can be integrated in national frameworks implementing the EU Toolbox. Measures may be implemented through national and/or EU-level actions, depending on the specific measure/actions. Some measures may be directly introduced or reinforced at national level (e.g. as part of the existing regulatory framework and powers of competent authorities), while others may require further action or joint action at EU level, in line with the respective competences. In selecting which measures are necessary to pursue, individual Member States will decide on the suitability of the measure. The Member State will also need to assess whether it has the resources to enforce the measure or if there is a need to cooperate with other Member States or at EU level.

3.3. Regarding strategic measures (SM) recommended in the EU Toolbox:

- **SM01 - Strengthening the role of national authorities**
  - *Guidance for the implementation of SM01 for Open RAN deployments:* National authorities should use regulatory powers to be able to scrutinise large-scale Open RAN deployment plans from MNOs and if needed, restrict, prohibit and/or impose specific requirements or conditions, following a risk-based approach, for the supply, large-scale deployment and operation of the Open RAN network equipment.
  - This assessment should take into account, among other things:
    - Whether MNOs have adequate controls to be able to manage the increased complexity of system integration and operation of Open RAN networks, and to achieve mature processes and appropriate network management capabilities;
    - Whether the components used follow, once available, the relevant Open RAN technical specifications, and whether security controls are implemented in these technical specifications.

- **SM02 – Performing audits on operators and requiring information**
  - *Guidance for the implementation of SM02 for Open RAN deployments:* National competent authorities should require MNOs to provide detailed and up-to-date information about their plans for the sourcing of Open RAN equipment and the involvement of third party suppliers (system integrators, cloud service/infrastructure providers, etc.). Adequate design and deployment plans, including risk analysis and possible mitigation plans, should be provided to support effective auditing in modular and dynamic Open RAN scenarios.

- **SM03 - Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks - for key assets**
  - *Guidance for the implementation of SM03 in Open RAN deployments:* This assessment and related restrictions should include Open RAN suppliers, external service providers related to Open RAN, cloud service/infrastructure providers and system integrators. The profile of all stakeholders - including new actors - should be carefully assessed. This assessment should take into account the criteria recommended in the EU Coordinated risk assessment, which cover the risk of interference from a non-EU country, the supplier's ability to supply and the overall quality of products and cybersecurity practices of the supplier.

- **SM04** - **Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support**
  - *Guidance for the implementation of SM04 for Open RAN deployments:* Controls and restrictions on MSPs should be extended to Open RAN providers, notably cloud service/infrastructure providers and system integrators. Trusted third parties providing network management services, such as MSPs and system integrators, can help in mitigating risks related to the combination of components from different suppliers and potential issues related to their interoperability. The risk profile of these third parties should be assessed in the same way as equipment suppliers, based on the criteria recommended in the EU Toolbox.

- **SM05** - **Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies**
    - *Guidance for the implementation of SM05 for Open RAN deployments:* National competent authorities and MNOs should consider the broader value chain beyond 5G when assessing dependencies and diversification in 5G networks. MNOs should have an appropriate multi-vendor strategy in their networks, and should include hardware providers, system integrators and cloud service/infrastructure providers to ensure that the risk of vendor lock-in is not increased. National competent authorities and MNOs can perform risk assessments to prevent cross-sector dependencies on a single cloud service/infrastructure provider. Measures to ensure interoperability and portability for migration of cloud providers would further mitigate the risks[20].

- **SM08 - Maintaining and building diversity and EU capacities in future network technologies**
    - *Guidance for the implementation of SM08 for Open RAN deployments:* EU and national funding for 5G and 6G R&D should be used to support opportunities for EU players to compete on a level playing field. MNOs should be encouraged to set up sustained programmes that involve EU players, including new entrants, in their Open RAN trials and deployments. In 6G, open and interoperable architectures can be designed from the outset.

3.4. As regards technical measures (TM) recommended in the EU Toolbox:

- All of the technical measures remain essential, in particular **TM03 (Ensuring strict access controls)**, **TM04 (Increasing the security of virtualised network functions, ensuring implementation of adequate security measures for all virtualised RAN components)** and **TM07 (Reinforcing software integrity, update and patch management)** require attention in Open RAN.
- In view of the challenges arising from Open RAN, some technical measures will need to be further reinforced and more strictly implemented and audited:

- **TM05 - Ensuring secure 5G network management, operation and monitoring**
    - *Guidance for the implementation of TM05 for Open RAN deployments:* MNOs should adapt the monitoring design to modular environment where each component is monitored, i.e. zero trust mind set.

- **TM09 - Using EU certification for 5G network components, customer equipment and/or suppliers' processes**
    - *Guidance for the implementation of TM09 for Open RAN:* The future candidate certification scheme for 5G should incorporate Open RAN components from the earliest possible stage.

- **TM10 - Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services)**
    - *Guidance for the implementation of TM10 for Open RAN deployments:* Consider the use of the future EU certification scheme for cloud to get assurance about the implementation of cloud services, e.g. transparency requirements on the location of servers and of key people such as administrators.

[20] Measures can include evidence of support of cloud interoperability together with data and application portability, as described by ISO/IEC 19941:2017 (Information technology — Cloud computing — Interoperability and portability, https://www.iso.org/obp/ui/#iso:std:iso-iec:19941:ed-1:v1:en), as well as actual proofs of MNOs cloud multi-provider strategies.

3.5. Regarding supporting actions (SA) recommended in the EU Toolbox:

- **SA01 - Reviewing or developing guidelines and best practices on network security**
  - *Guidance for the implementation of SA01 for Open RAN deployments:* Based on ENISA's report on NFV security[21], integrate NFV security controls in the 5G Security Controls Matrix, which is currently being developed by ENISA. In a second step, assess whether Open RAN controls need to be added to the Matrix. In addition to the updated technical guidelines on security measures under the European Electronic Communications Code (EECC)[22], assess whether additional guidance for national competent authorities on Open RAN is needed.

- **SA02 - Reinforcing testing and auditing capabilities at national and EU level**
  - *Guidance for the implementation of SA02 for Open RAN deployments:* National competent authorities and operators should consider applying for EU funding to develop common 5G penetration testing/redteaming capabilities[23].

- **SA03 - Supporting and shaping 5G standardisation**
  - *Guidance for the implementation of SA03 for Open RAN deployments:* All O-RAN specifications should be publicly available and the standardisation process should satisfy the World Trade Organisation (WTO)/Technical Barriers to Trade (TBT) founding principles for the development of international standards[24]. The current lack of transparency could be partially mitigated when O-RAN Alliance specifications are submitted for review and adoption by a European SDO, such as the European Telecommunications Standards Institute (ETSI). In the context of such transfer and adoption process like ETSI's ongoing Publicly Available Specifications (PAS)[25], Member States should coordinate in order to address security deficiencies and related requirements, and ask the O-RAN Alliance to give a commitment or indication as to when the organisation expects to submit the above specifications to ETSI for review. The O-RAN Alliance is particularly encouraged to ensure openness in participation and consensus and impartiality in decision-making. This will allow to increase transparency and ensure the representation of a wider set of stakeholders, including European ones, to implement a security-by-design approach and allow for effective security assessments that are in line with the principles of EU Regulation 1025/2012. Alternatively, these discussions can take place within the 3GPP, which has demonstrated to be the key forum on mobile standardisation, ensuring a balanced participation of worldwide stakeholders and SDOs.

[21] ENISA Network Function Virtualisation Security in 5G, Challenges and Best Practices, 24 February 2022, https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

[22] ENISA Technical Guideline on Security Measures Under the EECC report, 10 December 2020, https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc and ENISA 5G Supplement to the Technical Guideline on Security Measures Under the EECC report, 10 December 2020, https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc

[23] The DIGITAL Europe work programme for 2022 foresees a call on testing and certification capabilities to notably support cybersecurity and interoperability testing capabilities on 5G disaggregated and open solutions.

[24] Recital (2) of the Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation.

[25] In November 2021, the O-RAN Alliance submitted three specifications to ETSI for adoption as ETSI Technical Specifications or Technical Recommendations in the framework of ETSI's PAS procedure. The specifications are: O-RAN Fronthaul Control, User and Synchronization Plane Specification v7.01-Nov 2021 (ORAN-WG4.CUS.0-v07.01); O-RAN Open Fronthaul Management Plane Specification v7.01-Nov 2021 (ORAN-WG4.MP.0-v07.01.docx), and O-RAN Management Plane Specification -YANG Models 7.0 -March 2021 (O-RAN.WG4.MP-YANGs-v07.00).

- **SA06 - Exchange of best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers**
    - *Guidance for the implementation of SA06 for Open RAN deployments:* Exchange best practices on the application of strategic measure 03 to Open RAN stakeholders, notably on the definition of the key assets in Open RAN networks.

4. Key findings and conclusion

4.1. As concluded in the EU Coordinated risk assessment of 2019, 5G networks built with established models (non-Open RAN) present a significant and expanded threat surface compared to 4G networks, in particular due to their function of backbone to other critical infrastructures and the increased role of software and third-party suppliers. To address these risks, the EU agreed on a Toolbox of mitigating measures in January 2020, currently being implemented by Member States.

4.2. Building on the coordinated work already done at EU level to strengthen the security of 5G networks, this report looks at the security implications of Open RAN, which will offer an additional way of deploying the radio access part (RAN) of 5G networks in the coming years, alongside established architectures. There is still considerable uncertainty regarding scenarios of Open RAN deployment in the short and medium term.

4.3. The report found that the development of Open RAN technical specifications is underway and the consideration of security implications is still at an early stage. Overall, the report identifies a number of security challenges associated to Open RAN networks. At the same time, Open RAN may also bring opportunities to improve the security of the RAN, provided that certain conditions are met.

4.4. The EU Toolbox recommends that each operator has an appropriate multi-vendor strategy to avoid or limit any major dependency on a single supplier. Through greater interoperability among RAN components from different suppliers, Open RAN holds perspectives for allowing greater diversification of suppliers within networks in the same geographic area. In addition, Open RAN could also bring improvements as regards:

- Visibility of the network thanks to the use of open standards[26] and open interfaces, which could also facilitate auditing and security testing;
- Automation through the introduced intelligence in Open RAN which could help to decrease threats related to human error (This is a general trend in the evolution of network technology, not exclusive to Open RAN);
- Virtualisation and cloud-based solutions which allow for greater flexibility and make managing network resources easier (This is a general trend in the evolution of network technology, not exclusive to Open RAN).

4.5. However, since the Open RAN concept is still under development and its security at an early phase of maturity, the extent to which security opportunities will materialise is not yet clear, as they are associated with a number of conditions and counter-risks. As regards diversity of the supply chain, it is still uncertain whether Open RAN multi-vendor interoperability based on open standards[27] and open interfaces will be reached in the medium term, if indeed there will be a market with a choice of different RAN components from different suppliers, and to what extent MNOs will choose a mix and match approach using multiple RAN component suppliers. For operators, at least in the short run,

[26] While considering point 3.5. 'Supporting Action 03' and point 4.9 on addressing deficiencies in the development of technical specifications.

[27] While considering point 3.5. 'Supporting Action 03' and point 4.9 on addressing deficiencies in the development of technical specifications.

deploying Open RAN brings additional complexity, which requires additional technical expertise and more security assurance.

4.6. This analysis found that cybersecurity is a significant challenge for the Open RAN concept in general, and in particular O-RAN specifications still need to reach maturity in this area. Especially in the short term, by introducing a new approach, new interfaces and new types of RAN components potentially coming from multiple suppliers, Open RAN would exacerbate a number of the security risks of 5G networks and expand the attack surface in the radio access part of the network. The severity of these risks will vary depending on the market impact of Open RAN and the scale of its deployment by MNOs.

4.7. Specifically, key risks that are amplified or brought by Open RAN include:

- More entry points for malicious actors, irrespective of the supplier, due to a potentially increased number of suppliers and components;
- An expanded threat surface and a more complex environment leading to higher risks of vulnerability or failure, which could also lead to undesirable data and information flow to new third-party applications;
- An increased risk of misconfiguration of networks;
- Technical specifications, such as those developed by the O-RAN Alliance, not sufficiently mature and secure by design, and deficiencies in the O-RAN Alliance governance;
- New or increased dependency on cloud service/infrastructure providers, as virtualisation and the use of cloud is becoming more widespread in the telecoms sector, in particular in Open RAN deployments;
- New potential risks and impact on other network functions due to resource sharing and in case of not sufficient controls in place.
- The risk profile of a (potentially higher number of) individual suppliers continuing to be an important source of vulnerabilities.

4.8. In addition, by increasing momentum for new market players, including large non-EU players, Open RAN could have major disruptive impacts on EU capacities in the 5G supply market. This could lead to new critical dependencies in the medium to long term or to increasing existing ones (e.g. in the area of components and cloud) and weaken the EU's strategic autonomy and security.

4.9. To mitigate these risks and leverage potential opportunities brought by Open RAN, it is essential to implement the EU Toolbox measures to secure 5G networks. In addition, for networks based on Open RAN, further actions are required to extend or reinforce some of the EU Toolbox measures. These include:

- Using regulatory powers to be able to scrutinise large-scale Open RAN deployment plans from MNOs and if needed, restrict, prohibit and/or impose specific requirements or conditions for the supply, large-scale deployment and operation of the Open RAN network equipment;
- Reinforcing key technical controls such as authentication and authorisation, and adapting the monitoring design to a modular environment where each component is monitored;
- Assessing the risk profile of Open RAN providers, external service providers related to Open RAN, cloud service/infrastructure providers and system integrators, and extending the controls and restrictions on MSPs to those providers;
- Addressing deficiencies in the development of technical specifications: the process should satisfy the WTO/TBT founding principles for the development of international standards[28] and security deficiencies should be addressed;

[28] Recital (2) of the Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation.

- Including Open RAN components into the future 5G cybersecurity certification scheme, currently under development, at the earliest possible stage.

4.10. As regards preserving and consolidating EU capacities in this market, a technology neutral regulation to foster competition should be maintained. In this framework, EU and national funding for 5G and 6G R&D could be used to support opportunities for EU players to compete on a level playing field. Beyond the RAN, it is also important to address potential dependencies or lack of diversity across the whole communication value chain for the diversification of supply.

4.11. Overall, a cautious approach to moving towards this new architecture is recommended. Any transition from and coexistence with existing, reliable technologies should be done by allowing sufficient time and resources to assess risks in advance, implement appropriate mitigations and clearly define responsibilities in case of failure or incident. While looking for cost/performance trade-offs through Open RAN, MNOs and other stakeholders should pay sufficient attention to ensuring security, which may require significant investments, on top of existing 5G security measures.

5. Annexes

Annex 1. Security risks of Open RAN

This table lists the 9 risks already identified in the 2019 EU Coordinated risk assessment, with an estimation of the impact of Open RAN on this risk (amplified, similar, reduced) and its rationale. New risk categories and new risks are indicated in red. For each new risk, an illustrative risk scenario is proposed.

Risk category: Insufficient security measures		
Risk title	**Impact of Open RAN**	**Assessment**
R1. Misconfiguration of networks	Amplified	The fact that more components from different suppliers need to be integrated together, the use of virtualisation management and the lack of mature MNO processes for complete lifecycle of Open RAN deployment greatly increase configuration complexity and the risk of misconfiguration of networks and render faults more likely. Moreover, the lack of mature standards can lead to dissimilar and potentially poorer network design and architecture which increases the risk for ineffective emergency and continuity mechanisms. Decoupling hardware and software, and using software component from different suppliers present potential additional risk of misconfiguration of networks. Software may offer security feature, which relies on hardware implemented secure element, or security feature which requires support from other software component. As there may be many different combinations of software and hardware, or combinations of software components, integrating the security features may require additional effort and could easily end up to situations in which security features are not used.
R2. Lack of access controls	Similar or amplified	The increased number of Open RAN suppliers also means an increasing number of third parties needing access to the network (e.g. in case of malfunction). The new functions (for example xApps and rAPPs) will introduce new suppliers in the ecosystem and will require additional security controls and measures to be put in place between each and every function to avoid new security threats being introduced. MNOs may need to outsource the operations to third parties given the increased complexity and additional interfaces in Open RAN deployments. The use of open interfaces also increases the risk of a third party accessing the system.
New Risk (NR) 1. Expanded threat surface and vulnerabilities in Open RAN functions and interfaces	N/A (New risk)	The increased number of components in Open RAN deployments, potentially from multiple suppliers, together with new network functions as well as additional Lower Layer Split (LLS) interfaces, increase the attack surface. Also, the implementation of network functions with AI and ML introduces new attack vectors, for example through flaws in the ML model or via the interface to external sources (such as weather data). For instance, the O-RAN Alliance specifications, in their current version, include the possibility for external, potentially untrusted, sources to provide data to intelligent RAN functions and to configure the network intelligently, but these interfaces have not been further defined/described. Vulnerabilities in these interfaces and intelligent functions could negatively impact the network. In addition, by opening certain interfaces, Open RAN will give access to information flows to new third-party applications, which raises security issues with regard to

		data passing through the network. The O-RAN specifications already define capacities for opening certain interfaces to third-party applications. These openings aim to introduce new functionalities, but these third-party applications will have access to information flows (e.g. real-time location data of users connected to the network). **Risk scenario:** Adversary exploits insecure open fronthaul interface to mount denial of service, interception or tampering attacks, compromising availability, confidentiality, integrity or privacy of data. Alternatively, attackers may exploit weak authentication mechanisms to gain unauthorised access, compromise privacy, degrade network performance or facilitate attacks on other parts of the network[29].
Risk category: 5G supply chain		
Risk title	**Impact of Open RAN**	**Assessment**
R3. Low product quality	Amplified	Open RAN means that there will be more suppliers and more different components, potentially including components from high-risk suppliers. This means that the risk of diverse levels of quality product increases. It is unclear whether newcomers in the Open RAN market might prioritise innovation or security in the short-term. In addition, there may be suppliers whose maturity of software development, software security and supply chain security is lagging behind with respect to more established suppliers. A compounding factor is the fact that Open RAN standards are still under development and lacking maturity. This means that Open RAN products may lack a foundation of security-by-design. Considering that these components are interconnected, additional controls will be needed to avoid that these weakest links put other components and the other RAN functions at risk.
R4. Dependency	Reduced	An increased number of available suppliers, coupled with a disaggregated RAN, interoperable interfaces, an increased use of COTS hardware and possibly open source software could reduce the overhead in switching suppliers, allowing operators to reduce the potential for dependency on any single suppliers (See also under 'Supplier diversity in the RAN' in annex 2).
NR2. New dependency on cloud service/infrastructure providers in Open RAN	N/A (New risk)	A potential (and likely) implementation of Open RAN's modular approach for the RAN functions, and the disaggregation of software from hardware, enables (part of) the base station software to be run on cloud platforms, which could increase dependency on cloud service/infrastructure providers. As different suppliers may use different cloud platforms, there is a risk that the network becomes dependent on multiple cloud service/infrastructure providers at the same time. There is a possibility that the cloud service or part of it is run outside the EU where different legislation may apply. There may be also situations where all MNOs in a region end up using the same cloud provider. In this case, even if each of the MNOs has its own network, all the networks are relying on the same cloud provider, which could then exacerbate vulnerabilities. **Risk scenario**: Mobile network operators rely entirely on a small number of (mostly non-EU) cloud service/infrastructure providers for their Open RAN network supporting critical infrastructure, which creates a supplier lock-in.

[29] This scenario is also valuable in established networks but can be amplified as it applies to new open interfaces present in the Open RAN architecture.

NR3. Decreased sustainability of the EU 5G supply chain and potential dependencies on non-EU capacities	N/A (New risk)	The RAN supply market could be transformed in a way that gives momentum to new players (e.g. system integrators, cloud service/infrastructure providers, etc.), including large non-EU players. This could lead to new critical dependencies in the mid- to long term, or increase existing ones[30], with potentially significant impacts on security. **Risk scenario:** New business models based on Open RAN architectures and interfaces gain momentum and new major players enter the market, competing with the established players. The market could reconsolidate around a small number of non-EU suppliers, system integrators and cloud providers, thus negating the diversification opportunity.
NR4. Deficiencies in the O-RAN technical specifications development process	N/A (New risk)	Security has not been at the forefront of the technical specifications development process of the O-RAN Alliance[31] [32]. Immature O-RAN specifications without a foundation of secure by design may lead to products with increased vulnerabilities leading to exploitation. The lack of mature security specifications in a diverse Open RAN architecture coupled with increased competition can result in poorly manufactured components in an attempt to reduce cost. In addition, key decision rights within the O-RAN Alliance are conferred to the Board, which is composed only of a sub-set of members and only of MNOs. The participation in the specification development of the O-RAN Alliance seems to narrow as the process advances. The combination of conditions for document access and for membership seems to imply that while the documents may eventually be accessed by anyone, conditions to access specifications are more stringent for non-members and non-contributors. The stringent provisions of the O-RAN Alliance Adopter License Agreement might hamper the transfer of information and knowledge between adopters and non-adopters, making discussions outside the O-RAN Alliance more difficult. **Risk scenario:** O-RAN specifications continue to be developed in a setting which does not provide much visibility and openness to relevant stakeholders, and a lack of parity with the 3GPP international standardisation efforts. This weakens efforts towards ensuring a coherent secure architecture, can fragment the overall system security and create vulnerabilities in availability, integrity, confidentiality and privacy.
Risk category: Modus operandi of main threat actors		
Risk title	**Impact of Open RAN**	**Assessment**
R5. State interference through 5G supply chain	Similar	As there will be more suppliers in an Open RAN deployment (including possibly more high-risk suppliers), the potential exposure to a higher number of supply chain risks increases. The risk profile of a supplier - linked to the criteria identified in the EU Coordinated risk assessment (including the risk of interference by third country) - continues to be an important source

[30] High technology dependence has been identified in a number of areas, such as on components and cloud (Strategic dependencies and capacities, 5 May 2021, SWD(2021) 352 final).

[31] Open RAN Risk Analysis, commissioned by the German Federal Office for Information Security (BSI), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5GRAN-Risk-Analysis.pdf?__blob=publicationFile&v=7

[32] However, it should be noted that the O-RAN Security Focus Group has been established within the O-RAN Alliance to retroactively include security design specifications that are in parity with existing 3GPP architecture.

		of vulnerabilities. In addition, risks could exist also in relation to the source/actors providing inputs and data for the specification of open interfaces (see also NR.4 Deficiencies in the O-RAN technical specifications development process).
R6. Exploitation of 5G networks by organised crime	Amplified	The increased number of interfaces and suppliers would offer more opportunities for OCGs to enter and disrupt the network. In addition, smaller suppliers, such as those providing software services, may be more susceptible to be influenced by OCGs (or state actors). Moreover, the possible use of open source components could mean that the vulnerabilities are publicly-known and could therefore be more easily exploited by malicious actors.
Risk category: Interdependencies between 5G networks and other critical systems		
Risk title	**Impact of Open RAN**	**Assessment**
R7. Significant disruption of critical infrastructures or services	Similar or amplified	Identified risks related to Open RAN (in particular new vulnerabilities related to an increased number of suppliers and new interfaces which translate into a higher risk of exposure to network-level attacks compared to the established access network implementations) and the lack of fully mature security controls around Open RAN architecture and NFV mean that critical national infrastructures relying on 5G networks could also be more exposed to incidents. .
R8. Massive failure of networks due to interruption of electricity supply or other support systems	Similar	This risk can affect the RAN, and the impact would depend on the split of functions in the 3GPP or Open RAN specifications. In case of power supply disruption, a network using a distributed architecture could be impacted at a larger extent due to the physical distance that exists between the physical equipment/hardware hosting central unit (CU) and/or distributed unit (DU) functionalities. It is therefore important to ensure that adequate energy back-up sources are installed in multiple physical points in order to protect service availability in a single/particular area.
Risk category: End-user devices		
Risk title	**Impact of Open RAN**	**Assessment**
R9. IoT exploitation	Similar	Open RAN components, the network functions running on them, but also for example virtualised MEC applications, would be vulnerable to attacks from connected terminals, such as IoT devices, but the risk would be similar for network components in an established RAN architecture.
New risk category: Interoperability and management		
NR5. Open RAN network fault management complexity	N/A (New risk)	Failure in specific network components built by a specialised supplier may impact the entire network. Multiple suppliers may increase complexity and cost of managing network services and fault management, by making it more challenging to discover the cause of network failures or by requiring (remote) support provided by several different suppliers, hence increasing the risk. In addition, more Open RAN suppliers could mean it is harder to allocate and enforce liability to one or more suppliers.

		Risk scenario: An unintentional system failure in one of the critical components built by a specialised supplier and the complexity of identifying and resolving the issue in the multi-vendor set-up impacts the availability causing prolonged outage of network services.
NR6. Impact of Open RAN mix and match approach on network security and performance	N/A (New risk)	Integration of multiple supplier components into a single network, in particular in the lack of a mature standard, which by its nature enables efficient interoperability, can cause integration problems, prevent specific security controls to function or make it more difficult to conduct network testing. Moreover, an increasingly complex environment with multiple components from different suppliers and with multiple stakeholders involved makes it more challenging to ensure that only trusted and competent individuals are involved in network deployment, operation and maintenance. Additionally, the increased number of components and interfaces and/or the application of necessary resource-demanding protection mechanisms on those elements may also lead to degradation of overall performance or prevent specific use-cases dependant on performance such as ultra-reliable low latency communications (URLLC). Furthermore, the ability of the MNO to pursue a systematic approach to security controls across the network is impeded by a diversity of security mechanisms. In addition, different releases of the same software might be deployed in a heterogeneous way. **Risk scenario:** Unintentional human error in operating and managing complex network environment or an intentional malicious action by a non-trustworthy third-party personnel with high access privileges lead to unavailability of network services or facilitate further attacks on other parts of the network.
NR7. Resource sharing	N/A (new risk)	In Open RAN, different network functions are virtualised and are running on the same hardware, which means that potentially, if there are not sufficient controls in place, other network functions could be impacted by security issues with other new RAN functions running on the same pool of resources. **Risk scenario:** If one non-critical network function is running alongside other network functions on the same pool of hardware resources, then a security incident affecting the non-critical network function, for example an overload or distributed denial-of-service (DDoS) attack, could impact the security of other network functions.

Annex 2. Security opportunities of Open RAN

This tables describes some potential security opportunities that Open RAN could bring, under the condition that a number of factors are gathered. Moreover, some counter-risks are associated with these potential opportunities.

Title	Description	Level of potential benefit	Enabling factors	Counter-risk(s)
Security opportunities increased by Open RAN				
Supplier diversity in the RAN	Open RAN could play a role in increasing diversity of RAN suppliers and contribute to a more competitive market environment. This could in turn contribute to reducing dependency on high-risk suppliers, since more suppliers would be generally available on the market.	High	• Mature, robust and highly standardised open interfaces. • Level of acceptance of standards by industry and national authorities. • Presence and market share of non-high-risk suppliers.	• Re-consolidation of market. • Decreased sustainability of the EU 5G supply chain and potential dependencies on non-EU capacities. Increased complexity and exposure area due to the number of interfaces and risk of security failure in a single 'weakest link' product. • Priority to innovation and free-rider attitude of new entrants reducing incentives to invest in security. • Dependencies deeper in the supply chain of critical components (e.g. chips) may still exist.
Interoperability	A higher amount of components with open interfaces increases interoperability in the RAN. Open RAN could also bring more flexibility and dynamic networks, with the ability to swap components out as required without costly and long entire RAN replacement.	High	• Degree of maturity and use of open standards. • Level of acceptance of standards by industry and national authorities. • Key role of the system integrator to guarantee interoperability.	• Risk of market reconsolidation. • Risks related to greater role of system integrator. • Challenges for interoperability testing and maintenance of releases due to increased number of suppliers.

				• Ambiguities regarding liability issues may cause delays, for example in network repair measures.
Visibility and auditing	The use of open standards (see Supporting Action 03) for open interfaces between RAN components means that RAN components from different suppliers connect with each other in a similar way. This makes it easier for auditors and security testers to understand how a certain RAN implementation is working. The use of open standards also enables the broader community of experts to collaborate and work together on security and vulnerabilities. The increased use of open source in Open RAN could similarly allow for greater visibility and transparency about how systems work.	Medium	• Amount of open source software used for Open RAN. • Level of maturity of Open RAN definitions and specifications. • Commitment of Open RAN suppliers to security and global security assurance schemes. • Full publication of specifications of the open interfaces. • Auditing and security testing capabilities. • Technical knowledge of auditors. • Quality and security of the open source products. • Certification schemes for RAN components.	• Complexity (more components, more suppliers, in addition to integrators) could make auditing more difficult and resource-intensive for national authorities. • Open source is not a guarantee for better security. Vulnerabilities may exist in both closed and open source software.
Role of EU-based suppliers	Open RAN could bring new opportunities for EU suppliers, including SMEs and start-ups, to specialise in some areas and play a role in the Open RAN market. Already established EU suppliers could be well placed to take on the role of system integrators.	Medium/Low	• O-RAN specifications deficiencies need to be addressed and need to include all stakeholders, in order to create a level playing field for all players, including new entrants.	• Decreased sustainability of the EU 5G supply chain and potential dependencies on non-EU capacities.
Security opportunities present in but not specific to Open RAN				
Automation	The introduced intelligence in Open RAN can be used to automate the management and control via big data analysis, AI and ML. As a consequence,	Medium/Low	• Intelligent applications (xApp, rApp), AI and ML techniques, advanced functionalities leveraging RIC and Service	• Additional security and availability risks can be generated by automation processes and can affect

	closed loop responses to changes in the network can be automatically performed. This has the potential advantage that the need for human interactions may be reduced, which may decrease threats related to human error (e.g. accidentally altering the security posture of a network function).		management and Orchestration (SMO) should be used in an efficient way.	important segments of the network. • MNOs can lose insight, knowledge and control of critical processes such as change management and incident management, in particular, when the AI is only defined by its interfaces, and its implementation and training model remain closed. This could result in unpredictable network behaviours that MNOs cannot easily or quickly rectify. • The applications (xApp, rApp) enabling more automation in the RAN have access to sensitive attributes. Their compromise would give an attacker access to valuable information and new ways to take down the network.
Cloudification and virtualisation	Open RAN is likely to accelerate the adoption of virtualisation and containerisation and the use of open source and/or COTS hardware. Virtualisation and cloud-based solutions allow for greater flexibility and control of networks. Due to the modularity, operators can tailor their deployments and shift more easily the resources for monitoring and control to meet better these requirements.	Medium/Low	• Security controls for NFV (whether technical or more broadly organisational/operational) should be in place, carefully considering the network function criticality and sensitivity of information it handles. • Security in the entire COTS product lifecycle, including that it follows security requirements in the relevant standards (e.g. 3GPP and ETSI) should be ensured.	• Security challenges associated with virtualisation and cloud related to: implementing and operating virtualisation and containerisation (e.g. handling hypervisor-related vulnerabilities); secure orchestration and management; a need for effective and secure administration and access controls; incorporating new and legacy technologies; managing risks related to open source software and COTS hardware.

			• Standardisation process for the RAN hardware and the hypervisor would be needed to avoid lock-in into one specific set of products, specifications or technology.	For instance, open source software can provide attackers with a target-rich environment due to its widespread use. COTS hardware, on the other hand, may not have uniform security controls in place. Once it is compromised, the software running on it will be compromised as well, for example by way of manufacturing backdoors eavesdropping, inducing faults, and hardware modification tampering through jailbroken software.

Annex 3. Mitigating measures

This table lists the main EU Toolbox measures which are particularly important for Open RAN deployments and how they could be extended or reinforced to mitigate the risks identified in the report.

STRATEGIC MEASURES				
Id	**Measure**	**Guidance on the implementation of the EU Toolbox measure for Open RAN deployments**	**Related risks**	**Relevant actors[33]**

SM01	**Strengthening the role of national authorities**	• National authorities should use regulatory powers to scrutinise large-scale Open RAN deployment plans from MNOs and if needed, restrict, prohibit and/or impose specific requirements or conditions, following a risk-based approach, for the supply, large-scale deployment and operation of the Open RAN network equipment.
		• This assessment should take into account, among other things:
		  ○ Whether MNOs have adequate controls to be able to manage the increased complexity of system integration and operation of Open RAN networks, and to achieve mature processes and appropriate network management capabilities;
		  ○ Whether the components used follow, once available, the relevant Open RAN technical specifications, and whether security controls are implemented in these technical specifications.
			R1, R2, R3, R4, R5, R6, R7	• Relevant authorities
				• Operators

SM02	**Performing audits on operators and requiring information**	• National competent authorities should require MNOs to provide detailed and up-to-date information about their plans for the sourcing of Open RAN equipment and the involvement of third-party suppliers (system integrators, cloud service/infrastructure providers, etc.). Adequate design and deployment plans, including risk analysis and possible mitigation plans, should be provided to support effective auditing in modular and dynamic Open RAN scenarios.	R1, R2, R3, R4, R5, R6, R7, NR5, NR6	• Relevant authorities • Operators
SM03	**Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk - including necessary exclusions**	• Include Open RAN suppliers, external service providers related to Open RAN, cloud service/infrastructure providers and system integrators in this assessment and related restrictions. The profile of all stakeholders - including new actors - should be carefully assessed. This assessment should take into account the criteria recommended in the EU Coordinated risk	R2, R5, NR1, NR4	• Relevant authorities • Operators

[33] This column aims at identifying the main owners of the measures, i.e. actors responsible for developing, enforcing and/or implementing a measure.

	to effectively mitigate risks - for key assets	assessment, which cover the risk of interference from a non-EU country, the supplier's ability to supply and the overall quality of products and cybersecurity practices of the supplier.		
SM04	**Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support**	• Controls and restrictions on MSPs should be extended to Open RAN providers, notably cloud service/infrastructure providers and system integrators. Trusted third parties providing network management services, such as MSPs and system integrators, can help in mitigating risks related to the combination of components from different suppliers and potential issues related to their interoperability. The risk profile of these third parties should be assessed in the same way as equipment suppliers, based on the criteria recommended in the EU Toolbox.	R2, R5, NR5	• Relevant authorities • Operators
SM05	**Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies**	• National competent authorities and MNOs should consider the broader value chain beyond 5G when assessing dependencies and diversification in 5G networks. MNOs should have an appropriate multi-vendor strategy in their networks, and should include hardware providers, system integrators and cloud service/infrastructure providers to ensure that the risk of vendor lock-in is not increased. National authorities and MNOs can perform risk assessments to prevent cross-sector dependencies on a single cloud service/infrastructure providers. Measures to ensure interoperability and portability for migration of cloud providers would further mitigate the risks[34].	R4, NR2	• Relevant authorities • Operators
SM08	**Maintaining and building diversity and EU capacities in future network technologies**	• EU and national funding for 5G and 6G R&D should be used to support opportunities for EU players to compete on a level playing field. MNOs should be encouraged to set up sustained programmes that involve EU players, including new entrants, in their Open RAN trials and deployments. In 6G, open and interoperable architectures can be designed from the outset.	R4, NR2, NR3	• EC and Member States • All 5G stakeholders

[34] Measures can include evidence of support of cloud interoperability together with data and application portability, as described by ISO/IEC 19941:2017 (Information technology — Cloud computing — Interoperability and portability, https://www.iso.org/obp/ui/#iso:std:iso-iec:19941:ed-1:v1:en), as well as actual proofs of MNOs' cloud multi-provider strategies.

TECHNICAL MEASURES				
Id	**Measure**	**Guidance on the implementation of the EU Toolbox measure for Open RAN deployments**	**Related risks**	**Relevant actors**
TM05	**Ensuring secure 5G network management, operation and monitoring**	• MNOs should adapt the monitoring design to a modular environment where each component is monitored, i.e. zero trust mind set.	R1, R2, R3, R5, R6, R7, R9, NR5, NR6	• Relevant authorities • Operators
TM09	**Using EU certification for 5G network components, customer equipment and/or suppliers' processes**	• Incorporate Open RAN and its components, from the earliest possible stage, in the future candidate certification scheme for 5G.	R3, R6, R7, NR4	• Relevant authority • EC • ENISA • Stakeholders
TM10	**Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services)**	• Consider the use of the future EU certification scheme for cloud to get assurance about the implementation of cloud services, e.g. transparency requirements on the location of servers and of key people such as administrators.	R9, NR4	• Relevant authority • EC • ENISA • Stakeholders
SUPPORTING ACTIONS				
Id	**Measure**	**Guidance on the implementation of the EU Toolbox measure for Open RAN deployments**		**Relevant actors**
SA01	**Reviewing or developing guidelines and best practices on network security**	• Based on ENISA's report on NFV security[35], integrate NFV security controls in the 5G Security Controls Matrix, which is currently being developed by ENISA. • Assess whether Open RAN controls need to be added to the Matrix. • In addition to the updated technical guidelines on security measures under the European Electronic Communications Code (EECC)[36], assess whether		• Relevant authorities • ENISA • Operators

[35] ENISA Network Function Virtualisation Security in 5G, Challenges and Best Practices, 24 February 2022, https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

[36] ENISA Technical Guideline on Security Measures Under the EECC report, 10 December 2020, https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc and ENISA 5G Supplement to the Technical Guideline on Security Measures Under the EECC report, 10 December 2020, https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc

		additional guidance for national competent authorities on Open RAN is needed.	
SA02	**Reinforcing testing and auditing capabilities at national and EU level**	• National competent authorities and operators should consider applying for EU funding to develop common 5G penetration testing/redteaming capabilities[37].	• Relevant authorities • EC • ENISA
SA03	**Supporting and shaping 5G standardisation**	• All O-RAN specifications should be publicly available and the standardisation process should satisfy the WTO/TBT founding principles for the development of international standards[38]. The current lack of transparency could be partially mitigated when O-RAN Alliance specifications are submitted for review and adoption by a European SDO, such as the ETSI. In the context of such transfer and adoption process like ETSI's ongoing PAS[39], Member States should coordinate in order to address security deficiencies and related requirements. To further facilitate this, Member States could also ask the O-RAN Alliance via the PAS process to present the end-to-end security solutions and mechanisms specified or planned for the Open RAN solution together with the time plan for the release of associated specifications and, based on this information, ask the O-RAN Alliance to give a commitment or indication as to when the organisation expects to submit the above specifications to ETSI for review. The O-RAN Alliance is particularly encouraged to ensure openness in participation and impartiality in decision-making. This will allow to increase transparency and ensure the representation of a wider set of stakeholders, including European ones, to implement a security-by-design approach and allow for effective security assessments that are in line with the principles of EU Regulation 1025/2012. Alternatively, these discussions can take place within the 3GPP, which has demonstrated to be the key forum on mobile standardisation, ensuring a balanced participation of worldwide stakeholders and SDOs.	• Relevant authorities • EC • Operators • Suppliers • ENISA

[37] The DIGITAL Europe work programme for 2022 foresees a call on testing and certification capabilities to notably support cybersecurity and interoperability testing capabilities on 5G disaggregated and open solutions.

[38] Recital (2) of the Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation.

[39] In November 2021, the O-RAN Alliance submitted three specifications to ETSI for adoption as ETSI Technical Specifications or Technical Recommendations in the framework of ETSI's PAS procedure. The specifications are: O-RAN Fronthaul Control, User and Synchronization Plane Specification v7.01-Nov 2021 (ORAN-WG4.CUS.0-v07.01); O-RAN Open Fronthaul Management Plane Specification v7.01-Nov 2021 (ORAN-WG4.MP.0-v07.01.docx), and O-RAN Management Plane Specification -YANG Models 7.0 -March 2021 (O-RAN.WG4.MP-YANGs-v07.00).

SA06	**Exchange of best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers**	• Exchange best practices on the application of strategic measure 03 to Open RAN stakeholders, notably on the definition of the key assets in Open RAN networks.	• Relevant authorities