OECD publishing

ENHANCING THE SECURITY OF COMMUNICATION INFRASTRUCTURE

OECD DIGITAL ECONOMY PAPERS

September 2023 **No. 358**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report on “Enhancing the Security of Communication Infrastructure” was prepared jointly by the OECD Working Party on Security in the Digital Economy (WPSDE) and Working Party on Communication Infrastructure and Services Policy (WPCISP), of the Committee on Digital Economy Policy (CDEP). It aims to inform policy makers about the current challenges and opportunities related to the digital security of communication networks. In parallel with the development of this document, the WPSDE and WPCISP developed reports on the “Security of the Domain Name System (DNS): an Introduction for Policy Makers” and on “Routing security: BGP incidents, mitigation techniques and policy actions”.

This report was drafted by Lauren Crean and Ghislain de Salins with contributions from Laurent Bernat, Verena Weber and by WPSDE and WPCISP delegates. It was prepared under the supervision of Laurent Bernat and Verena Weber. This paper was approved and declassified by written procedure by the Committee on Digital Economy Policy on 31 May 2023 and prepared for publication by the OECD Secretariat.

The Secretariat wishes to thank the external experts who contributed to the development of this report including, inter alia: Amy Alvarez, Chris Boyer and Jason Olson (AT&T); Eric Wenger (Cisco Systems); Claire Milne (CSISAC), Carolina Botero and Andrés Velásquez (Fundación Karisma, CSISAC); Judith Furlong and Said Tabet (Dell Technologies); ENISA, the European Union Agency for Cybersecurity; Jason S. Boswell, Mikko Karikytö, Scott Poretsky and Rene Summer (Ericsson); the European Commission; Kathryn Condello (Lumen Technologies, Inc.); Chelsea Smethurst and Mark Svancarek (Microsoft); Roopa Prabhu (Nvidia); Alexander Botting (Open RAN Policy Coalition); Leonid Burakovsky and Alex Hinchliffe (Palo Alto Networks); Brian Larkin (National Telecommunications and Information Administration), Brandon Moss and Katie Mellinger (Federal Communications Commission), and Jonathan Murphy (Department of Homeland Security) (United States).

Note to Delegations:
This document is also available on O.N.E under the reference code:
DSTI/CDEP/CISP/SDE(2021)3/FINAL

Executive summary

Communication networks are the foundation of the digital transformation. Given their crucial role, **digital security and resilience have become a priority for policy makers** across the OECD to ensure the functioning of our digitally dependent economies and societies and strengthen trust in the ongoing digital transformation. However, cyberattacks on these networks are on the rise and increasingly sophisticated. At the same time, communication networks are undergoing significant changes and are being upgraded to new technological standards (e.g. 5G and 6G), which, in turn, impact their security.

This report considers four trends that are shaping and changing communication networks and the digital security implications these raise:

- The **increasing criticality of and reliance on communication networks** by the economy and society, which is changing the context of digital security of communication networks.
- An **increased virtualisation of networks and a more important use of cloud services.**
- A **shift towards more openness in networks**, including open radio access network (RAN).
- The role of **artificial intelligence in communication networks**.

Each of these trends is shaping communication networks and, therefore, prompts questions on their implications on digital security.

On the one hand, **these trends benefit digital security risk management** of communication infrastructure. They can help improve network visibility and management, enable network segmentation and isolation, allocate security resources more effectively, and automate the early detection of malware and malicious activity. Increased transparency and reduced dependencies on certain suppliers are additional possible benefits to digital security, driven by the shift towards more openness.

However, **these trends also challenge digital security risk management** in communication infrastructure. Overall, they result in:

- An **expanding attack surface** (i.e. the set of points of an information system that are potentially vulnerable to an attack). Since the architecture of communication networks is increasingly complex, and because networks are increasingly software-defined, cloud-based and virtualised, they contain more software vulnerabilities that can be exploited.
- A **broader and more complex supply chain**. Some of the technological advancements outlined in the trends tend to increase the dependency of network operators on some of their suppliers and to redistribute control and responsibility for the management of digital security risk along the entire value chain. These suppliers include providers of telecommunication equipment, as well as providers of cloud, components, servers and managed services, which are likely to play an increasingly important role in the digital security of communication networks. The communication infrastructure supply chain is often complex, which makes the allocation of responsibility in case of a digital security incident even more difficult.

- An **aggravating threat landscape**, driven in part by the commoditisation of attacks (e.g., "ransomware-as-a-service") and the increasing sophistication of State-sponsored and other threat actors. Against this backdrop, malicious actors' motivation to breach communication networks' availability, integrity or confidentiality is significantly increasing as communication networks become increasingly critical.

The paradox facing governments is that while communication networks are increasingly considered critical infrastructure, their digital security ultimately depends upon decisions made by third parties, namely network operators and their suppliers. Nevertheless, **governments do have a clear role to play** to incentivise the adoption of digital security best practices and to support an enabling environment that empowers stakeholders to reach an optimal level of digital security. This can be fostered through the following policy objectives:

- First, **adopting a holistic and strategic approach** towards enhancing the digital security of communication infrastructure**,** which i) considers the entire lifecycle of products and services on which operators rely, ii) gathers all relevant stakeholders and iii) is co-ordinated across the whole government and at the international level. Importantly, **co-ordination across governmental agencies** and a clear definition of responsibility and/or mandates between them are essential.
- Second**, incentivising network operators to enhance digital security** and adopt comprehensive risk management frameworks (i.e., risk assessment and risk treatment) and encouraging them to explore more advanced security approaches, such as the "zero trust" model.
- Third, **addressing supply chain digital security risk** by incentivising suppliers to improve supply chain transparency (e.g. through enhanced traceability of components and digital security certification) and supporting diversification within information and communication technology and services supply chains.

These three objectives can help structure public policy interventions to improve the digital security of communication infrastructure. Governments can apply **several policy actions** to address the cross-cutting challenges and uphold policy objectives, ranging from light-touch to more interventionist approaches**: voluntary frameworks and guidance, multistakeholder initiatives and funding research, third-party evaluation and certification, public procurement, and legal requirements**. These actions can be shaped as needed to carefully address the cross-cutting challenges in terms of scope, scale and speed of cyberattacks. OECD countries have introduced policy initiatives spanning these policy actions, from voluntary frameworks to legal requirements on digital security. However, digital security is an ever-moving target that requires constant re-evaluation, both regarding the best practices available for private stakeholders to implement as well as the structure and objective of public policies to create the enabling environment to incentivise the adoption of best practices by private stakeholders.

Table of contents

Tables

Figures

Boxes

Enhancing the security of communication infrastructure

Introduction

Communication networks are a key foundation of the digital transformation of the economy and society. Given their crucial role, as evidenced by the COVID-19 pandemic, ensuring their digital security has become a priority for policy makers across the OECD. Enhancing the digital security and resilience of these networks is critical to ensure the functioning of our digitally dependent societies and strengthen trust in the ongoing digital transformation. This is especially important as our interconnected economies face increasing endogenous and exogenous risks, exacerbated by geopolitical tensions and conflicts (OECD, 2021[1]).

As most critical sectors have become reliant on digital technologies, the impact of digital security attacks on operators of critical activities has increased significantly. In the past few years, malicious actors have disrupted key industries such as gasoline and fuel distribution (Colonial Pipeline), healthcare (Irish Health Service Executive), finance (Reserve Bank of New Zealand), food production (meat supplier JBS), energy (Ignitis Group) and postal services (Royal Mail) (ZDNet, 2021[2]; Government of Ireland, 2021[3]; Reserve Bank of New Zealand, 2022[4]; BBC, 2021[5]; LRT, 2022[6]; The Guardian, 2023[7]).

In this context, communication network operators have developed multiple solutions and partnerships to better manage digital security risk, for instance by establishing communication-specific Computer Emergency Response Teams (CERTs) and Information Sharing and Analysis Centres (ISACs). However, they also fall victim to cyberattacks that exploit vulnerabilities in their information systems and networks, or through their supply chains. For example, the Mirai malware incident in 2016 demonstrated the possibility of leveraging poorly secured Internet of Things (IoT) devices to form a botnet and launch Distributed Denial-of-Service attacks (DDoS) (OECD, 2021[8]). One malware based off the Mirai source code disrupted more than 900 000 Deutsche Telekom (DT) routers, limiting DT's clients' ability to access the Internet (OECD, 2021[8]).

Malicious actors may also specifically target the communication sector in order to gain access to sensitive customers' data. For instance, security researchers uncovered targeted attacks on the communication industry in Southeast Asia in 2021 ("DeadRinger"), as well as an advanced persistent threat (APT) group targeting communication operators identified in 2018 ("Operation Soft Cell") (Cybereason Nocturnus, 2021[9]; White House, 2021[10]). In both cases, security researchers suspect the attackers' aim was to obtain sensitive data, such as call data records.

Scope

This report aims to analyse the digital security implications of key trends that are affecting communication network infrastructure.[1] The scope of the report is limited to *public* communication networks, i.e. networks

used primarily for the provision of publicly available communication services. Unless specified otherwise, the term "communication networks" therefore refers to "public communication networks" in the report.

Private networks, including private clouds, are outside the scope of this report. Such private networks may range from an individual customer's local area network (LAN) to an organisation's intranet or to a private 5G network deployed by a large organisation (e.g. Nornickel, a mining company in Australia (AMSJ, 2021[11])). Those private networks are typically not subject to the same regulatory regime that applies to public communication networks.

In addition, while there are different ways to transmit communication signals (for instance, terrestrial, submarine cable, satellite), this report does not discuss the specific security implications of one mode of transmission.

Several stakeholders are responsible for the digital security of communication networks. At a high level, these can be grouped into three broad categories:

- **End users** of communication networks ("Users"), including individuals, businesses and governments that use public communication services to carry out economic and social activities;
- **Operators** of communication networks ("Operators"), which provide public communication services to end users or deliver traffic in the provision of these services. This category includes Internet Service Providers (ISPs) (e.g., Orange or Vodafone), and backbone Internet providers (e.g., Lumen, Comcast);
- **Actors of the operators' supply chain ("Suppliers"):**
    - Suppliers of software and hardware used in communication networks, including, for example:
        - Suppliers specifically offering communication hardware equipment and associated services, such as Cisco, Ericsson, Huawei, Nokia, Samsung or ZTE;
        - Other more generic hardware and software suppliers.
    - Service providers, including, for example:
        - Managed service providers (MSPs), including for digital security (e.g. FireEye, Palo Alto Networks);
        - Cloud service providers (e.g. Microsoft Azure or Amazon Web Services);
        - Content delivery networks (CDNs) (e.g., Akamai or Cloudflare);
        - System integrators, which facilitate the deployment of suppliers' products in operators' networks (e.g. Capgemini, NEC, Parallel Wireless).

In this report, the term "supplier" includes the direct suppliers of operators as well as *their* suppliers. While end users have some responsibility for managing digital security risk, they are outside the scope of this report.

These categories are not meant to be exhaustive and they may overlap (e.g., some businesses fall into several categories). For instance, one operator could also provide certain services to another operator, becoming part of its supply chain, such as in the case of a large ISP providing transit services to another ISP (carrying the traffic of a customer ISP for a fee) or settlement-free peering (carrying traffic of another ISP free of charge, on a reciprocal basis).

The report provides an overview of four key trends, both technical and non-technical, that are impacting the digital security of communication network infrastructure. Although other trends may impact communication networks in the future, such as quantum computing, the report focuses on those currently shaping them today. The report analyses the security implications of these trends and discusses how policy makers can best address them.

Digital security of communication networks

Digital security, which is often referred to as cybersecurity or information security, is usually defined as the set of measures organisations take to manage digital security risk. Digital security risk is the detrimental effect that digital security incidents can have on economic and social activities. In this report, a digital security incident is an intentional or unintentional event that can disrupt the availability, integrity and confidentiality ("AIC triad") of data, information systems and communication networks, and as a consequence, negatively impact the economic and social activities that rely on these networks:

- **Availability**: the communication network is not accessible and usable on demand by authorised users;
- **Integrity**: the communication network, or the data transiting over it, have been altered in an unauthorised manner;
- **Confidentiality**: unauthorised entities have access to the data transiting over the network.

Digital security attacks, also known as cyberattacks, are incidents that are intentionally caused by malicious actors, such as a Denial-of-Service (DoS) attack affecting the availability of the network for a few hours or days (Security Boulevard, 2021[12]). A ransomware attack would usually affect the whole AIC triad, as the encrypted data would no longer be available on-demand for authorised users, and likely would have been accessed and/or altered by unauthorised users. On the other hand, some attacks may affect only the confidentiality of data, and may therefore be more difficult to detect as they do not alter availability. Unintentional incidents include, for instance, a power outage, a flood or a human error.

Digital security incidents result from a combination of vulnerabilities and threats. Vulnerabilities are weaknesses in software, hardware, networks or data whose exploitation would lead to an incident. They include, *inter alia*, flaws in the code of software or hardware products used by network operators, misconfigurations of equipment or software, human error (e.g. an employee susceptible to phishing) or poorly managed access controls. Much of the public debate surrounding 5G security focuses on vulnerabilities in network equipment that could be inserted intentionally ("backdoors") by State-sponsored entities (Bloomberg, 2019[13]). However, this is only a fraction of vulnerabilities that can be exploited as products that contain code almost always contain –"unintentional"– vulnerabilities. For example, on average, 40 new code vulnerabilities are discovered every day in widely used products such as iOS, Windows or Android (OECD, 2021[8]; OECD, 2021[14]).

Threats include malicious actors willing to exploit vulnerabilities to cause harm and the tools and techniques ("vectors") they use to carry out attacks (e.g. "malware"). Malicious actors range from relatively unskilled individuals and attackers with ideological motivations to more sophisticated groups including organised crime and State-sponsored actors, which can benefit from quasi-unlimited resources and are often referred to as "APTs". State-sponsored attacks are generally pursuing geopolitical goals, while cybercriminals are primarily seeking financial gains. Key trends in this area include:

- A sharp rise in ransomware attacks, whose objective is to extort money from various types of organisations, from businesses to hospitals (OECD, 2020[15]);
- The commoditisation of cybercrime tools, now largely accessible "as-a-service" or "on-demand" (Dark Reading, 2019[16]); and
- The increasing sophistication of attacks, resulting in part from State-sponsored offensive capabilities. Examples of large-scale sophisticated attacks include the SolarWinds intrusion campaign (FireEye, 2020[17]).

Most experts agree that the evolution of the global threat landscape increases the overall level of digital security risk and affects all organisations, regardless of their size and location. This evolution also affects the availability, integrity and confidentiality of communication networks, which could seriously impair the functioning of the whole economy and society (NIS Cooperation Group (EU), 2020[18]).

As a result, there has been a growing awareness among policy makers of the need to better understand and manage the digital security of communication networks. However, many publications tend to focus either on the technical aspects of digital security or on national security concerns. The purpose of this report is to go beyond these two angles and to favour a holistic approach, focusing on economic and social aspects. Approaching digital security primarily from the national security perspective typically leads to a focus on threats[2] (in particular, foreign States and associated States-sponsored actors), while overlooking vulnerabilities and resilience. However, while economic actors, such as operators and suppliers, have little leeway to influence the behaviour of threat actors, they can mitigate vulnerabilities for which they are responsible (see below) and take measures to reduce the impact of potential incidents and increase resilience.

For both policy makers and organisations, effective digital security policies should aim to manage digital security risk rather than to entirely avoid it (e.g. by going offline or slowing down the digital transformation). A key challenge is that digital security measures usually impact other aspects of business operations, for instance costs, performance or usability. As there may be trade-offs, network operators and their suppliers should seek to reach an optimal level of digital security, e.g. in alignment with stakeholders' risk tolerance and regulatory requirements, rather than "100% security". In addition, as the risk is constantly evolving with new vulnerabilities and threats constantly appearing, digital security should be considered an ongoing process, rather than a definite state.

A brief description of communication networks

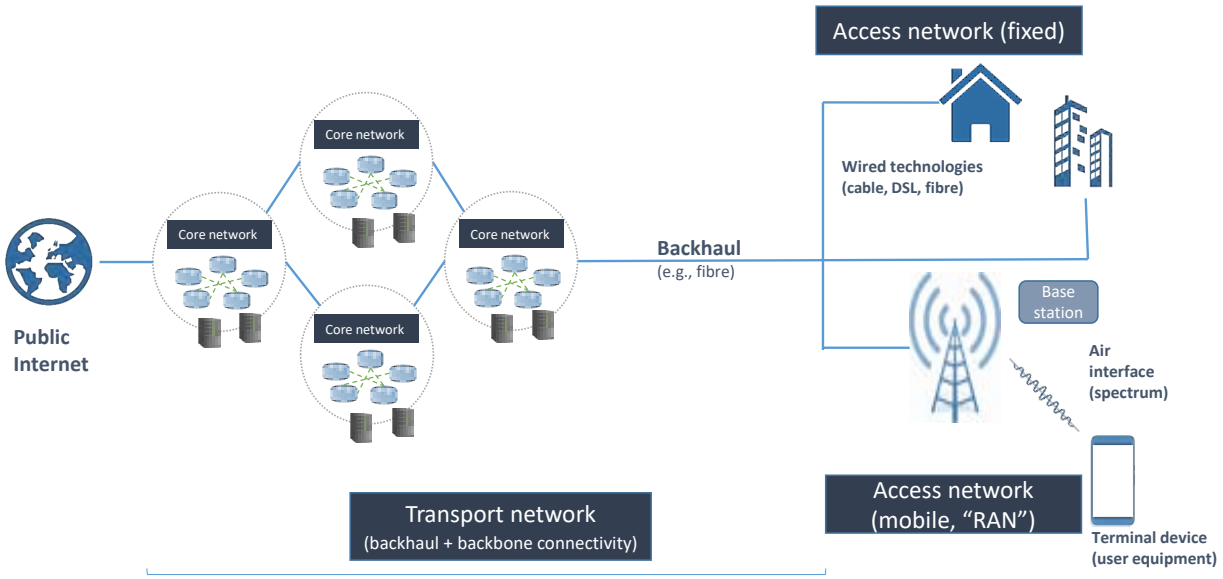
Communication networks can be seen as transmission systems that enable the exchange of information in an analogue or digital way. These networks can include, for example, broadband (fixed or mobile) networks, the Internet, which is a network of networks, or legacy public telecommunication networks, such as the public switched telephone network (PSTN).

The architecture of communication networks can be broken down into three distinct parts:

- the **access network** (also commonly referred to as 'last-mile')
- the **transport network (including backhaul)**, and
- the **core network**.

The access network is the part of the communication network that connects subscribers to their communication service provider. In fixed networks, the access network connects to end users' devices through wired technologies such as copper, cable and fibre. For mobile networks, the access network is referred to as the radio access network (RAN), which connects to end users' devices using spectrum (see Figure 1). Backhaul infrastructure forms the transport network, connecting the core networks to the access networks. The core network, which may also be called "backbone", exchanges information and connects nodes within the network. When considering telephony, the core network directs calls over the PSTN; when considering IP packets, the core network exchanges packets quickly between different network nodes. Communication networks are interconnected in order to provide end-to-end communication between end users with different operators. Interconnection can take place directly between two communication networks or at Internet exchange points (IXPs), which can be seen as bulk traffic exchange crossroads where multiple networks such as ISPs, CDNs, and content providers exchange traffic.

Figure 1. High-level overview of communication network architecture



Source: OECD elaboration, based on information from Figure 1 in European Court of Auditors (2018[19]), *Broadband in the EU Member States: despite progress, not all the Europe 2020 targets will be met*, https://op.europa.eu/webpub/eca/special-reports/broadband-12-2018/en/.

Communication networks' infrastructure is made up of software and hardware like routers, switches, middleboxes and servers:

- Routers connect two or more networks and act to manage traffic and forward packets;
- Switches allow multiple devices to connect and form a network;
- Middleboxes are devices that perform network-specific functions on traffic (for example, firewalls inspect traffic and apply access control policies);
- Servers manage higher-level network services, such as billing, telemetry, analytics, and operations control.

Servers are often located in data centres where they can rely on additional services such as cloud solutions for mobile edge computing.[3] Networking hardware, such as those defined above, are located throughout the whole infrastructure, from the core network, to the transport network, to Internet exchange points (IXPs) and to the access network.

Given the increasing convergence of mobile and fixed networks, this report discusses the trends affecting the digital security of fixed and mobile networks jointly, instead of evaluating each market separately. As Figure 1 shows, mobile networks can be thought of as an extension of fixed networks, with the distinction referring primarily to the last-mile access network, connecting to the end customer. In addition, mobile networks increasingly rely on fixed networks to meet demands on the network, through backhaul as well as offloading traffic from the mobile network to the fixed network through Wi-Fi offloading. For instance, 5G networks require fibre backhaul to support demands for high capacity and high speeds on its network (OECD, 2019[20]).

Trends in communication networks impacting digital security risk

This section presents and discusses four trends that are particularly important for the digital security of communication networks:

- The criticality of communication networks;
- The virtualisation of networks and the integration of cloud services into networks;
- The momentum towards openness; and
- The use of AI in communication networks.

Each section describes the trend and how it is changing communication networks, as well as a brief analysis of its main drivers, including economic incentives for industry adoption, where appropriate. Then, each section examines the key security benefits and challenges brought by the trend, to point governments to the key elements to consider when devising policy options on how to best accompany these trends.

Importantly, policy makers should keep the following nuances in mind when reading this report, including regarding the analysis of the security benefits and challenges that can be associated with each trend. First, the level of development of the trends analysed below may vary significantly, including across and within countries, and between different network operators. Some trends have already impacted communication networks and will continue to develop, whereas others are at an earlier stage, with the exact pace of their development uncertain. For instance, various scenarios are plausible regarding the short-term evolution of open networking architectures (e.g. open RAN) (European Commission, Directorate-General for Communications Networks, Content and Technology, Dinges, M., Hofer, M., Leitner, K., et. al., 2021[21]).

Second, the analysis of the security benefits and challenges should not be read as an argument on whether or not policy makers should support or prevent the development of these trends. The framing of these developments as “trends” underlines that they are already underway, and that their adoption is driven by the significant benefits they bring for the industry. Digital security is just one policy objective amongst others and should be balanced with other objectives such as economic development, quality of service, coverage, affordability of communication services and strategic autonomy, to name a few. Therefore, policy makers should focus on how to best accompany stakeholders throughout these changes and adjust policies accordingly, taking into account the impact of these trends on digital security risk.

Third, the level of development of these trends does not necessarily make communication networks more or less secure. In fact, the development of these trends may make some vulnerabilities more easily manageable, while making other vulnerabilities more prominent or more difficult to handle. More generally, the level of digital security of a communication network depends upon numerous factors, and many of them depend on the contexts of implementation, including across time (e.g. changing threats) and space (e.g. applicable law).

Overall, the development of these trends is likely to result in a shift of digital security risk. Whether this shift will result in higher or lower risk in the medium- to long-term will depend in part on how stakeholders will handle it and how threat actors will adapt to it, which is unknown. It is, however, essential to recognise and understand this shift to make appropriate risk management decisions at the operational and public policy levels.

Increasing criticality of communication networks

Digital transformation leads to a growing reliance of the economy and society on communication networks. The COVID-19 pandemic accelerated and illustrated the many benefits of the digital transformation, as digital technologies supported the resilience of individuals and businesses during the crisis (e.g., maintaining business continuity during stay-at-home orders). Fixed and mobile operators witnessed a surge in Internet traffic to meet the increased demand as more and more citizens of OECD countries began

working and studying from home due to mobility restrictions (OECD, 2020[22]). In the first quarter of 2020, some operators experienced up to a 60% increase in Internet traffic compared to pre-pandemic levels and various operators recorded increases in the use of videoconferencing tools, virtual private network traffic, messaging and content traffic (OECD, 2020[22]).[4] Internet traffic also grew by 58% on average among OECD countries from 2019 to 2020 (OECD, 2022[23]). OECD countries added over 21 million fixed broadband subscriptions over the course of 2020 which represents a 48% growth compared to average yearly additions from 2010 to 2019 (OECD, 2023[24]).

The increase in traffic and subscriptions also indicates a wider adoption of digital services, which are more and more intertwined with critical activities. For instance, the number of telemedicine appointments in France grew from around 40,000 in February 2020 to 5.5 million between March and April 2020 at the peak of lockdown restrictions (Eurohealth, 2020[25]). The United States similarly saw an increase in telehealth visits by 50% in the first quarter of 2020 compared to Q1 2019 and a peak increase of 154% in the last week of March 2020, compared to the same week in 2019 (Koonin et al., 2020[26]). While the circumstances surrounding the pandemic drove this growth, the benefits of increased convenience and access suggest it will continue to play a role in the delivery of health services. This is just one example of how the digital transformation makes other critical sectors (e.g. healthcare, transport, banking, energy) increasingly dependent upon the communication sector. While communication networks are usually considered as critical infrastructure in and of themselves, they are also interlinked to the functioning of other critical sectors. Therefore, any disruption in communication networks can have ripple effects in other critical sectors.

This dependence on communication networks across sectors is only expected to increase. In particular, the rollout of 5G networks is expected to enable new and advanced use cases in critical sectors of the economy and society, including healthcare, transport and manufacturing, which require low latencies, high network reliability, high capacity and high speeds. Many of these advanced use cases incorporate IoT devices, especially in critical sectors such as transport and healthcare, which will require the capability and reliability of 5G networks. Therefore, the amount of connected IoT devices relying on communication networks (especially 5G networks) is expected to increase exponentially as new use cases emerge that leverage the advanced capabilities. Communication networks are especially important to support these IoT applications for critical uses or sectors, as they typically have more stringent requirements for reliability, speed and capacity than can be guaranteed over Wi-Fi networks.[5] To support the requirements of these advanced use cases and increased number of devices, 5G networks require a significant amount of fibre backhaul to meet the speed and capacity demands on the network (OECD, 2019[20]). Therefore, both fixed and mobile communication networks play important roles in providing connectivity to support the digitalisation of other critical sectors.

Security implications

As most critical activities increasingly rely on communication networks to function, the potential impact of digital security attacks targeting communication networks is much higher now than it was several years ago and will continue to grow. For instance, a breach of the availability of communication networks could seriously impair the functioning of other critical activities, such as international trade or the provision of healthcare or energy, with cascading effects in other critical and non-critical sectors.

Cyberattacks on critical infrastructures are common and sometimes successful. In 2021, the United States' Colonial Pipeline incident led to fuel shortages across the East Coast, and the attack on the Irish Health Service Executive disrupted dozens of hospitals in the country. Hospitals around the world experience numerous ransomware attacks, some of which severely affect patients. In the United States, an Alabama woman whose baby died during a ransomware attack on the hospital where she was giving birth in 2019 has sued the institution for negligence and wrongful death (The Independent, 2021[27]). According to the US Cybersecurity and Infrastructure Security Agency (CISA), ransomware cyberattacks on hospitals lead

to significant and sustained hospital strain and related consequences (CISA, 2021[28]). In 2021, water supplies have also been targeted in the United States and France (NBC News, 2021[29]; Vitard, 2021[30]). In December 2015, 30 electricity substations were shut down by a cyberattack in Ukraine, leaving 230 000 customers without power from one to six hours (Wired, 2016[31]).

The interest of threat actors in targeting communication networks is growing. In recent years, communication network operators fell victim to a wave of ransomware attacks that hit many organisations across sectors and countries, in particular operators of critical activities. There have been reports of successful ransomware attacks on communication network operators, for example, in Argentina (ZDNet, 2020[32]) France (Forbes, 2020[33]), Korea (BBC, 2017[34]) and Sri Lanka (EconomyNext, 2020[35]). In these cases, the attacks were attributed to criminal groups motivated by financial gain and impacted the availability of information systems. However, in most of these cases, the impact was limited to internal information systems, and did not impact the availability of the networks and associated services to their customers.

Beyond criminal groups, the increasing dependency of critical activities over communication networks is expected to further attract State-sponsored actors and other military-grade groups, and the threat posed by such actors is expected to significantly increase in the coming years (ENISA, 2019[36]). In 2019, for example, a long-term, large-scale attack specifically targeted ten communication network operators across Europe, Africa and the Middle East. Operation “Soft Cell” was attributed to State-sponsored intelligence-gathering groups, also known as APTs (CSO, 2019[37]). The goal of the attack was to extract confidential information, and in this specific case, hundreds of gigabytes of data of call records were stolen. However, experts consider that as the attackers had gained full control of their targets’ information systems, they could have shut down entire mobile networks if they wanted to, hence impacting the availability of these communication networks’ infrastructure. Experts consider that in the coming years, APTs will increasingly seek to disrupt the availability of communication networks. The combination of motivation, intent, and a high-level capability enables States and associated actors to carry out very complex attacks on communication networks with major impact on critical activities, such as large-scale outages, or to attack interdependent critical activities, such as power supply, through communication networks (NIS Cooperation Group, 2019[38]). For the same reasons, terrorist groups are also likely to be increasingly interested in launching digital security attacks targeting communication networks specifically.

The scale of the impact that successful attacks on communication networks could have on the economy and society is both a powerful incentive for sophisticated threat actors and a growing concern for governments. There are many possible scenarios of large-scale disasters affecting communication networks, which are characterised by cross-sectoral dependencies. For example, the disruption of a major operator in a country would likely affect large parts of the economy because of downstream dependencies: the impact would cascade from the operator to its customers, whose activities would also be disrupted, on to their customers or users, and so on. Furthermore, some of these knock-on effects may also affect other critical sectors whose functioning depends upon it such as energy, transport and health care, whose operators may not have appropriate communication redundancy.

In another scenario, the same failure may affect several operators at the same time, for example if an attacker exploits a vulnerability in a common product or component used by operators. Such critical vulnerabilities have been found in several popular software and software libraries embedded in numerous products used across sectors. The Wannacry and NotPetya attacks, as well as Spectre and Meltdown vulnerabilities in microprocessors, provide examples of a single vulnerability, or group of vulnerabilities, that potentially affects large spans of the economy. Other examples include vulnerabilities grouped under names such as Amnesia:33, Urgent/11 and Ripple20, which in these cases affected TCP/IP libraries in widespread communication, IoT and industrial equipment (Armis, 2020[39]; Hacker News, 2020[40]; Wired, 2019[41]). The possible economic impact of such catastrophic scenarios has yet to be assessed, as models are difficult to develop given the complexity of dependencies and multiplicity of factors.[6]

Virtualisation of networks and the integration of cloud services

This section introduces two trends that are increasingly intertwined in today's communication networks: network virtualisation and the increased role of cloud services in communication networks.

Virtualisation of networks

Network virtualisation describes a shift from a hardware-dependent network to one that relies on software to handle network functions. Network virtualisation abstracts a machine's resources from hardware to software. It allows for the creation of virtual simulated environment(s) by separating a machine's resources from its physical hardware (e.g., the physical network) and making them available to these virtual environments, or to aggregate multiple physical networks into one virtual network (VMware, 2023[42]). In other words, virtualisation creates a software-based version of a piece of hardware such as compute, storage or networking components, servers, applications (IBM Cloud, 2021[43]). Network operators are applying virtualisation to their networks through network function virtualisation (NFV) and Software-defined networking (SDN). In mobile networks, NFV and SDN together enable network slicing (OECD, 2019[20]).

Network function virtualisation (NFV) and Software-defined networks (SDN)

NFV virtualises the different components of networks and SDN centralises network control. NFV decouples network functions from hardware appliances, allowing them to be run as software (OECD, 2019[20]).[7] With NFV network functions of a legacy (i.e. non-virtualised) network, such as firewalls, routing, load balancing, and traffic management, among others, are transformed into "virtualised network functions" (VNFs) and can run on virtual machines. Virtual machines (VMs), which have been around for several years, are one type of a virtualised environment that virtualises the physical hardware.[8] Another more recent and increasingly popular approach is to use containers, which virtualises the operating system rather than the hardware by leveraging the resources of the host operating system (OS) (IBM Cloud, 2021[43]).[9]

Both containers and VMs offer flexibility, scalability, cost benefits and less network downtime (IBM Cloud, 2021[43]). However, compared to VMs, containers are more lightweight and portable, and are well suited to microservice architecture and to cloud deployments, as they can be easily moved. However, VMs are more isolated from one another than containers, which share a host's OS, which has security implications. Nevertheless, networks can and are using both VMs and containers in conjunction to leverage the advantages of both (VMware, 2020[44]).[10]

Complementary to NFV, software-defined networks (SDN) separate the control plane from the forwarding plane (also referred to as user or data plane) in the network (SDxCentral Studios, 2016[45]). The control plane decides how packets (data) are sent from one point to another, while the forwarding plane sends or "forwards" the data (Cloudflare, 2023[46]). A single control panel can, for example, manage and define policies for the whole network.

NFV and SDN bring many benefits, including enabling efficient resource management, automation and centralisation. Separating hardware from software, as in NFV, allows infrastructure resources to be shared and reassigned more easily, and enables these resources to serve different virtualised network functions (ETSI, 2014[47]). This allows resources to be used more efficiently and provides the ability to scale network functions dynamically, in response to actual and changing demands seen on a network (ETSI, 2014[47]). The centralisation of control enabled with SDN reduces operational costs by automating software updates and policy changes across the network and introduces flexibility to quickly respond to changing business needs by deploying new application, services, and infrastructure through software updates (SDxCentral Studios, 2016[45]).

This trend can be applied broadly to network architecture and is not limited to only mobile networks. Software-defined access networks (SDAN) also leverage the benefits of SDN and NFV for fixed networks, which may lead to cost savings, better network management, and flexibility (Nokia, 2023[48]). Other

applications of network virtualisation can be seen in software-defined wide area networks (SD-WAN) as well as at lower layers of the transport network, for instance. Nevertheless, both NFV and SDN have been trialled for 4G networks but are expected to be especially important for 5G networks to allow for network slicing (OECD, 2019[20]).

Many operators recognise the benefits NFV and SDN bring to networking. For example, in 2020, Vodafone deployed NFV in its 21 European markets and is leveraging NFV and SDN to deliver cloud-based network functions (VMWare, 2021[49]). Vodafone estimates that its investment reduces the time to develop and deploy network functions by 40% and the cost savings of up to 55% (VMWare, 2021[49]).

Network slicing

Network slicing allows an operator to provide several logical service networks, called slices, over the same physical network infrastructure (OECD, 2019[20]). Network resources can be shared among the slices, providing the respective services with different performance characteristics to meet their respective needs (OECD, 2019[20]). Several performance characteristics could differ between network slices based on service requirements, including speed, latency, mobility, reliability, or level of security.

With network slicing, an operator can physically separate traffic through slices and each slice could be configured for a specific service, set of users or application (IBM, 2021[50]) . Network slicing has been discussed for some time and is possible on 4G networks (Ericsson, 2018[51]). In 5G networks, it is expected to provide the flexibility and more efficient use of resources to handle the diverse demands expected on the network.[11] Use cases for 5G networks are often broken into: i) enhanced mobile broadband (eMBB), including augmented and virtual reality; ii) massive machine type communication (mMTC), such as IoT use cases where a large number of connected devices with long battery lives send non-time sensitive data; and iii) ultra-reliable and low latency communication (urLLC), i.e. use cases that have strict performance requirements such as high capacity and availability and low latency such as autonomous cars and industrial automation (ITU, 2015[52]).

A key benefit of network slicing lies in its ability to use one physical network infrastructure to deliver different performance and quality of service characteristics, depending on the needs of that particular slice, and to charge customers according to the characteristics of the slice in question (OECD, 2019[20]). While networks are able to support different quality of service parameters without using network slicing, for instance to support high resiliency and availability for certain types of traffic, like emergency services, this can be accomplished more easily with network slicing.

The active implementation of network slicing in 5G networks remains a complex undertaking and is still in the beginning stages (Subedi et al., 2021[53]). However, anticipated benefits are encouraging network operators to implement it. Telefónica, together with the University of Vigo in Spain and Cisco announced a network slicing trial in February 2021, focusing on three slices dedicated to low latency, high bandwidth, and emergency cases, respectively (Telefónica, 2021[54]). Vodafone UK and UK Power Networks announced a partnership, whereby “smart substations”[12], which transform energy in the electricity grid, will communicate with each other over a dedicated, highly secure slice of Vodafone’s SA-5G network (Vodafone, 2021[55]). In Korea, KT announced the commercialisation of its Standalone (SA) 5G network, noting its plans to further develop 5G services for enterprise customers leveraging network slicing (KT, 2021[56]). In the United States, Verizon noted its aim to deploy network slicing where needed (Mobile World Live, 2021[57]).

The integration of cloud services in communication networks

Cloud services are used across different parts of the network. There are two simultaneous trends related to cloud technologies, which are discussed in the following sections. On the one hand, the use of the cloud is increasing to handle key network functions, including in the core of networks. On the other hand, more

cloud services are currently being deployed at the edge of networks and closer to the end-user, which is termed “multi-access edge computing” (MEC).

Cloud services

Cloud services rely on virtualisation and can be defined as “a service model for computing services based on a set of computing resources that can be accessed in a flexible, elastic, on-demand way with low management effort” (OECD, 2014[58]). A cloud *pools* resources, such as computing, networking and/or storage capacity, and makes them available to different users on-demand, providing increased flexibility and potential cost savings for cloud users compared to managing dedicated infrastructure (RedHat, 2018[59]).

Cloud architectures are complementary to and increasingly interwoven with SDN and NFV. SDN can manage cloud-based infrastructure and provides useful visibility and automation into the entire network, including in cloud environments. The flexibility and automation of SDN meshes well with cloud environments and the integration between enterprise SDN and cloud will likely continue. Furthermore, NFV infrastructure can all be hosted on the cloud.

A few key benefits of cloud services include flexibility and potential cost savings through the transformation of capital expenditures to operational expenditures. Cloud services give organisations the flexibility to quickly scale up or down their computing resources according to demand without having to own or maintain their own infrastructure.

Cloud services are well-established in communication networks and are considered a key enabler to support communication networks to meet demands for bandwidth, including for 5G networks. While operators have long recognised the benefits of leveraging cloud processing, storage and computing resources in their networks, they are now considering how cloud strategies can support their future needs, as an extension of their recent migration towards NFV architecture.

One emergent trend is the increased use of cloud services to manage key components of networks, as network functions are increasingly being integrated into the cloud. As cloud services become more important for communication networks, dedicated partnerships between communication operators and cloud providers have been emerging in recent years. Microsoft Azure, Google Cloud and Amazon Web Services (AWS) all have dedicated offerings targeting the communication industry, demonstrating the increasing role of the cloud in network operations and conversely, the industry’s growing importance for cloud providers (Microsoft Azure, 2020[60]; Google Cloud, 2020[61]; AWS, 2023[62]). While the offerings from each cloud provider may vary, most include solutions related to edge computing, cloud-native mobile solutions, network operations, and AI, machine learning, and data analytics. As shown in Table 1, operators are often engaging in partnerships with more than one cloud provider. Indeed, cloud providers’ targeted strategies suggest that they are actively competing for network operators’ business, although some may argue that the small number of global providers of cloud services may result in a lack of supplier diversity and increase the risk of lock-in due to challenges related to cloud portability.

Table 1. Selected partnerships between communication operators and cloud providers

Companies involved in partnership	Year	Description
Amazon, KDDI, SK Telecom, Verizon, Vodafone	2019	Launch of AWS Wavelength to bring AWS services to the edge of the 5G network.
AT&T, Google Cloud	2020	Development of 5G edge computing solutions for enterprise customers using AT&T’s 5G network and Google Cloud.
AT&T, IBM	2019	AT&T Business applications will migrate to IBM Cloud and IBM will help manage AT&T hybrid cloud infrastructure. AT&T Business named as primary provider of SDN at IBM.
AT&T, IBM	2020	Joint solution to offer hybrid cloud to enterprise 5G customers leveraging AT&T MEC and IBM Cloud.

AT&T, Microsoft	2019	AT&T is migrating non-network infrastructure application to Microsoft Azure. Microsoft will also support AT&T's consolidation of its data centre infrastructure and operations.
Bell Canada, Google Cloud	2021	Bell is shifting its IT infrastructure, network functions and critical applications from on-premise cloud to Google Cloud and leveraging Google Cloud's "Anthos for Telecom".
BT, AWS	2023	BT will use AWS Wavelength to power edge cloud services for its enterprise customers.
Lumen, Microsoft	2021	Lumen will integrate Microsoft Azure capabilities with Lumen's bare metal (physical HW) edge network, allowing customers to launch applications on Azure anywhere within its edge network.
NTT, Microsoft	2019	Development of a "Global Digital Fabric", solutions built on Azure, and next-generation technologies.
Orange, Google Cloud	2020	Orange plans to build a data analytics and machine-learning platform with Google technologies
Telefónica Germany, AWS	2020	Telefónica Germany will use AWS cloud infrastructure to virtualise 5G core, targeting industrial 5G applications.
Telefónica, IBM	2021	Collaboration on Telefónica's hybrid cloud services platform for enterprise customers ("Cloud Garden 2.0).
Telenet, Google Cloud		Telenet will use Google Cloud's, "Anthos for Telecom" in its data centres.
Telstra, AWS	2021	Integration of AWS' edge compute solutions in Telstra's multi-access network.
Verizon, AWS	2020	Verizon 5G edge with AWS is a cloud computing platform leveraging AWS compute and storage resources to allow Verizon customers to build/deploy new applications at the edge of the network.
Vodafone, Google Cloud	2021	Development of an integrated data platform to process and move large volumes of data into the cloud from different systems.

Source: OECD elaboration based on operator information including (in order): (AWS, 2019[63]); (Google Cloud, 2020[64]); (AT&T, 2019[65]); (IBM, 2020[66]); (Microsoft, 2019[67]); (Bell Canada, 2021[68]); (BT, 2023[69]); (Fierce Telecom, 2021[70]); (NTT, 2019[71]); (Google Cloud, 2020[72]) ; (Telefónica Germany, 2020[73]); (IBM, 2021[74]); (Telenet, 2021[75]) (AWS, 2021[76]); (Verizon, 2021[77]); (Vodafone, 2021[78]).

One example of the increasing level of partnership between providers of cloud services and operators can be seen in Microsoft's 2021 acquisition of AT&T Network Cloud platform technology, which AT&T had used previously to run cloud applications for its third-party customers. Under this arrangement, the Microsoft Azure for Operators cloud platform would support some of AT&T's network computing functions, including those previously handled by the operator's Network Cloud platform technology (Microsoft, 2021[79]). Microsoft also would develop tailored compute and storage capabilities for the operator. Along with the acquisition of its Network Cloud platform technology, Microsoft can also leverage AT&T's technical expertise to inform its offering tailored for communication operators (Microsoft, 2021[79]). For its part, AT&T aims to reduce cost, and leverage the cloud provider's edge network, AI technology, and cloud services to deliver new 5G services (AT&T, 2021[80]). Other similar cloud-related announcements include DISH's decision to build its standalone open RAN-based 5G network on AWS (Amazon, 2021[81]). Telefonica Germany plans to build its 5G core and network functions in AWS' cloud, specifically for industry-specific use cases (SDX Central, 2020[82]), with AWS virtualising the 5G core and developing network functions and Ericsson acting as the 5G core vendor and providing orchestration services. Finally, Telefonica announced plans to build an on-premise cloud in its data centres managed by Oracle, to support its mission-critical operational and commercial systems (Oracle, 2021[83]).

Multi-access edge computing (MEC)

Multi-access edge computing shifts cloud computing resources to the edge of the network to perform analysis, processing, and storage of data to reduce latency and increase performance of high-bandwidth applications (Juniper, 2020[84]). Previously referred to as mobile edge computing, MEC is access-agnostic ("multi-access"). It is expected to play an important role in 5G networks to handle expected demands on the network in terms of traffic and latency. For example, by enabling services and content caches to be placed at the network edge, local traffic can be handled efficiently, lessening congestion on the core network (ETSI, 2021[85]). In addition, computing at the network edge also allows for better observation of local demand and network conditions, which could include during cases of localised attacks.

MEC includes near edge compute, which is located in between the centralised core (e.g. centralised data centres at the operator), and far edge compute, which is nearest to the end user. Near edge and far edge

compute serve different purposes in network architecture and may require different levels of security and resiliency based on their placement within the network.[13]

MEC environments are characterised by a complex equipment ecosystem of diverse suppliers, vendors and stakeholders for both hardware and software devices, including infrastructure owners, service providers, system integrators and application developers (ETSI, 2021[86]).

While MEC has been deployed in 4G LTE networks, these solutions were developed as an add-on to existing networks and were largely self-contained (ETSI, 2018[87]). 5G networks, by contrast, are designed to facilitate and support different deployments of MEC from the start. As noted above, cloud providers recognise MEC's importance and have tailored offerings for edge computing (e.g., AWS Wavelength, Google Cloud 5G edge computing solutions, Azure for operators). As Table 1 demonstrates, there have been several recent partnerships related to edge computing between cloud providers and operators.

Security implications

Virtualisation and an increased use of cloud computing are interlinked technical trends that tend to cross-fertilise each other. It makes it difficult to precisely attribute security benefits and challenges to specific developments such as NFV and MEC. They bring considerable benefits for the industry and society (e.g. more efficient and redundant communication networks), as well as improvements in terms of security, as discussed just below. These benefits, which go well beyond digital security, are driving the adoption of virtualisation and cloud computing by the industry. However, they also result in new and significant digital security challenges, that policy makers should consider. Overall, and as discussed above, this section should be understood as a balanced presentation of the impact of virtualisation and cloud computing on the digital security of communication networks, rather than as arguments for or against their development.

Security benefits

Overall, virtualisation and the integration of cloud services can provide significant benefits for the management of digital security risk in communication networks. They are likely to facilitate vulnerability scanning, enable more visibility on the network (e.g. identification of assets, detection of potential threats), allow for a higher level of automation of security controls, a more efficient use and allocation of security resources (e.g. deployment of security updates, filtering) and better network segmentation through slicing and isolation. These benefits would significantly facilitate the implementation of the "defence-in-depth" principle and of a "zero trust" approach, which assume that a security incident has probably already occurred rather than only relying on perimeter bound security measures (for a more detailed discussion, see the section below entitled, "Exploring the potential of zero-trust approaches") More precisely, key security benefits from these technological evolutions include the following:

- Virtualisation has the potential to provide additional protection through isolation and containerisation. In fact, it is more difficult for malware and viruses to spread across isolated containers and machines (ENISA, 2020[88]). Each network function can be dedicated to a different container or virtual machine, with its own anomaly detection process. Virtual machines can provide a higher level of isolation than containers.
- SDN and NFV may allow for faster and facilitated scanning and patching of vulnerabilities (NIS Cooperation Group, 2019[38]). For example, container orchestration tools can make it easier to deploy security updates quickly and safely. A SDN controller can define and apply tailored security policies, provide more network visibility, allow monitoring at interfaces within the network for possible security breaches or anomalies, and collect data for analysis to tailor or update security policies.
- Network slicing can enable operators to tailor security controls differently for each slice, according to specific use cases.

- Cloud-based networks can be more resilient as they can allocate resources dynamically and flexibly, including filtering and traffic shaping, e.g. in case of a DDoS attack (ENISA, 2012[89]). They can also provide more redundancy. Physical security and access controls can also benefit from higher standards thanks to resource concentration (ENISA, 2012[89]).
- MEC allows network defenders to allocate security resources, such as threat monitoring and analytic tools, to where they are needed most: data can be scanned for security threats closer to where it originated, potentially allowing for faster remediation (CISA, 2020[90]).

The increasing role of world-spanning cloud providers such as Amazon, Google, Microsoft or Alibaba, in the design and management of communication networks comes with several benefits for managing digital security risk. Such companies provide on-demand access to cloud, networking and Internet services, and can provide highly scalable access to their infrastructures, for example, computing capacity and data centres (which is why they are sometimes referred to as "hyperscalers"). Contracting and partnering with such firms can enable operators to benefit from advanced digital security resources, as those actors have developed significant capabilities to manage growing complexity, including the overlay of multiple logical and physical layers and the development of far and near edge computing. Some communication network operators are partnering with such organisations because they often do not have such capabilities in-house. The digital security capabilities of large cloud providers often build on a specialised workforce with technical know-how and experience, economies of scale, a strong culture of risk management and innovation as well as the recognition of digital security as a key concern for their clients. For instance, partnerships between operators and cloud providers can enable a more efficient roll-out of security updates across software and firmware platforms and better threat monitoring across the communication network.

Security challenges

Virtualisation and an increased integration of cloud services bring considerable changes to the way communication networks are designed, deployed and operated, and to the actors that manage them. In particular, they result in an expanding attack surface, a growing complexity of network architecture and an increased role of infrastructure supply chain for digital security risk management.

The attack surface is significantly expanding

Overall, and as exemplified with 5G, communication networks are increasingly based on software, as opposed to "analogue" communication equipment that relied mostly on hardware[14]. As a result, the number of lines of code present in communication networks' infrastructure is considerably increasing, and the **attack surface** (i.e. the set of points of a system or network that are potentially vulnerable to an attack) of communication networks **is expanding significantly**. This increased attack surface derives from three factors, in particular:

- As the number of lines of code increases, more code vulnerabilities are inevitable (OECD, 2021[8]). With communication networks that are increasingly reliant on software, including for core network functions through NFV, SDN and MEC, a vulnerability in any software component can compromise the availability, integrity or confidentiality of the entire network. Virtualised environments are also subject to specific vulnerabilities that may not be present or significant in physical servers, such as hypervisor vulnerabilities or micro architectural vulnerabilities in processors (e.g. Intel Spectre/Meltdown).
- The supply chain of communication networks tends be complex and opaque. For instance, software products are rarely designed from scratch but rather built on commercial off-the-shelf (COTS) components and software libraries, including open source ones. In addition, operators may rely on different equipment providers and operate multiple generations of networks in parallel (e.g. 3G, 4G and 5G for mobile operators). This makes the assessment of the level of digital security of software products difficult, including for communication equipment (OECD, 2021[8]).

- Vulnerabilities may arise at various stages of the communication equipment lifecycle (OECD, 2021[8]):
    - A product can lack basic "security-by-design" features;
    - The producer may not have put in place effective vulnerability treatment policies, including for co-ordinated vulnerability disclosure (OECD, 2021[14]);
    - The network operator may have incomplete vulnerability management processes, including to deploy security updates. The more critical and complex the infrastructure, the more difficult it is to ensure effective patching, as updates need to be tested to reduce the likelihood that they introduce new security risk (OECD, 2021[14]);
    - The network operator may use legacy products that have reached their end-of-life (EOL), i.e. producers no longer support the product and will not patch any newly discovered vulnerability. The WannaCry attacks in 2017 highlighted the significant risk posed by the use of EOL products for critical functions such as operating systems (OECD, 2021[91]).

The increasing complexity of network architecture is a growing challenge for operators

The trends outlined above also make it more difficult for network operators to manage digital security risk because of the growing **complexity of network architecture**, as networks are increasingly made up of multiple logical and physical layers and involve a more diverse set of user categories, including Machine-to-machine (M2M) and IoT devices. Managing trust, identity and authentication across such a complex context is a key challenge for network operators, and significantly increases the risk of misconfigurations. In particular:

- Virtualisation and network slicing, specifically, require network operators to manage multiple configurations, increasing the likelihood of misconfiguration. Misconfigurations are a common type of vulnerability, and according to some estimates, one-third of successful attacks during 4G network testing were due to misconfigurations (Positive Technologies, 2019[92]). New types of vulnerabilities affecting the technologies used in SDN and NFV, including cloud systems and their configuration, are likely to appear. Possible data leakages between multiple virtual environments or slices are an increasing source of concern (NIS Cooperation Group, 2019[38]).
- MEC and cloud-based architectures can expose communication networks to new vulnerabilities, such as cross-contamination of shared resources. Edge computing facilities may be more vulnerable to physical attacks as they are geographically distributed and therefore more difficult to monitor continuously and protect against physical intrusion, theft and physical damages. As more sensitive functions move closer to the edge of the network, significant investments will also be required to move security controls to the edge as well (NIS Cooperation Group, 2019[38]). At the same time, the centralisation of network functions, enabled by virtualisation and cloud services, may create single points of failure. The complexity of MEC networks is also likely to make it harder for cloud providers to deliver the same level of security to their clients in hybrid environments as they can provide in public clouds.
- This increasing complexity may also hamper the effectiveness of incident response. Cascading failures in virtualised, monolithic, centrally managed cloud-based IT systems can be more difficult and time-consuming to manage than in systems built from standard network elements.

The role of network operators' supply chain for digital security risk is increasing significantly

The increased complexity of network architectures is likely to result in **the need for network operators to partner with third-party suppliers for managing digital security risk**. These suppliers include equipment, software and service providers such as cloud providers and managed service providers (MSPs) that handle network management functions or provide digital security services. More broadly, all suppliers that provide equipment whose disruption could affect the availability, integrity or confidentiality of their customers' infrastructure will have an increased role in managing the digital security of communication

networks. Suppliers of services that attackers could exploit to access or disrupt part of their customers' infrastructure are also likely to have larger role in digital security risk management, including for vulnerability treatment (OECD, 2021[8]).

The increased reliance of communication operators on suppliers results in a higher risk of falling victim to a supply-chain attack involving MSPs or critical software providers, making the risk profile of suppliers increasingly important in communication operators' risk assessments. The recent attacks against SolarWinds and FireEye showed that an attacker can target a single critical software to compromise thousands of its users, including in critical sectors (SolarWinds Corp., 2020[93]; The New York Times, 2020[94]). Attackers increasingly target these suppliers to exploit the privileged access they often have to their clients' information systems and to bypass most of these clients' digital security measures. In 2017, a pervasive cyberespionage campaign called Operation Cloud Hopper targeted at least a dozen MSPs to compromise their customers (Forbes, 2020[95]; PwC, 2017[96]). The ransomware attack on software provider Kaseya in July 2021 shows that criminal groups seeking financial gain can also carry out supply chain attacks. In this attack, threat actors compromised the update of a software used by MSPs to remotely manage their customers' networks, breaching the availability of these networks and disrupting activities of between 800 to 1 500 firms.

Besides the high-level challenges above, some stakeholders have also raised concerns regarding the impact of these technical trends on confidentiality, in particular with the software-based implementation of mechanisms to enable lawful access to operators' data. Such mechanisms could be used to circumvent end-to-end encryption and be abused by threat actors if improperly designed or managed (NIS Cooperation Group, 2019[38]). The global supply chains of communication networks are also likely to raise concerns regarding applicable law and conflicts of jurisdiction, for instance, if operators' data is stored within countries whose access to data rules are not interoperable. However, these concerns relate to the role of law enforcement authorities, which are outside the scope of this report.

To summarise, the virtualisation of networks along with an increased use of cloud computing tend to increase the attack surface of communication infrastructure and the complexity of their architecture, resulting in an increased role of suppliers such as integrators and cloud computing providers to manage digital security risk.

Towards more openness in networks

The concept of openness has strong roots in communication networks and Internet protocols and has been spreading across the industry. The openness and interoperability of the Internet protocol suite (e.g., TCP/IP) was one of the enablers to allow the Internet to scale to current proportions by providing a standard way to exchange information and is increasingly used as the main communication technology in recent mobile network generations. The latest trend towards more openness is moving away from networks based on proprietary hardware and software towards networks made up of more interoperable and software-defined components, made possible by some of the other trends outlined above.

The move towards more openness encompasses a shift from network architecture that is made up of a proprietary solution provided by a single or limited number of suppliers, to one that is to a greater extent made up of interoperable components provided by multiple vendors. From a hardware perspective, the move towards more openness can be seen in a migration from proprietary equipment towards more commodity off-the-shelf (COTS), standardised hardware. From a software perspective, openness may refer to open source software, which has been used for many years and has historically been a part of the trend towards more openness in communication networks (see Annex 1, Annex 1. Open Source Software in communication networks).

Other aspects of more openness in software include the open interfaces between network components and open application programming interfaces (APIs), which together with the openness of hardware, are

key elements of the trend towards more openness in communication networks. Importantly, these open interfaces and open APIs are based on industry-developed specifications. Such specifications and standards are developed in standards bodies such as the European Telecommunications Standards Institute (ETSI), 3rd Generation Partnership Project (3GPP) and the Internet Engineering Task Force (IETF), among others, as well as in other industry-led organisations, such as the O-RAN Alliance. The common set of technical specifications and standards provides the technical basis to support interoperability and fosters both the development of the equipment ecosystem and the deployment of new network architectures.

While these trends coincide, it does not mean that all software in an operator's network is open source, nor that every piece of hardware is from a different supplier or interoperable. In the case of open RAN, while additional open interfaces are defined, the software at the network component level can still be proprietary. Indeed, there are still many cases where operators use proprietary hardware or software from a specific vendor, based on each operator's preferences and specific network architecture.

Some of the motivating factors for operators to move towards more openness are, in general, more choice, modularity and flexibility in how they architect their networks. From a supply chain perspective, more choice and increased interoperability between network components (i.e. the ability to "mix-and-match" from different suppliers) allows for less dependence on one supplier and the option of a more diversified network equipment ecosystem. With the move toward commodity hardware and more open interfaces, new players can enter the market to supply these network components. This can promote competition with established players and drive innovation. A move towards more commodity hardware may result in lower prices, which may also be a result of greater competition. At the same time, network integration costs, due to increased complexity, may decrease the overall cost benefit that operators can expect.

To facilitate understanding, the trend is presented from two use cases: i) openness in information and communication technology (ICT) elements and networking hardware equipment in the core network, i.e. "open networking", and ii) openness in mobile networks, or "open RAN".

Open Networking

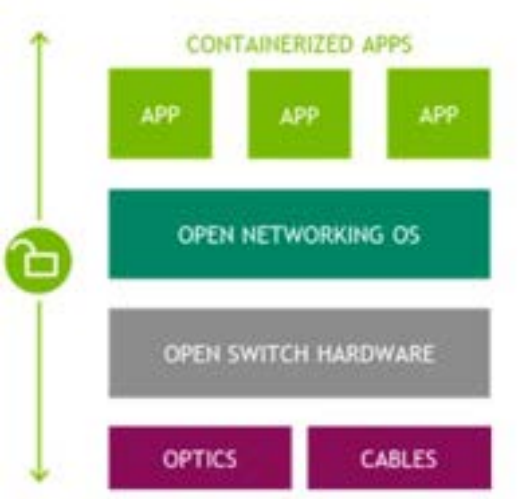
While the definition of open networking differs within industry, the main characteristics often include interoperability and network disaggregation, use of open standards, SDN principles, and open source software in network components. Nevertheless, for the purposes of this section, "open networking" considers the move towards openness in the core network. This includes ICT elements associated with the core network, such as data centres, servers, and networking hardware equipment such as routers and switches, as well as their software components (e.g., network operating system). While networking hardware equipment like routers and switches are located throughout communication network infrastructure (e.g., core network, backhaul, and access network), the focus will be those primarily found in the core network.

Examples of industry-led initiatives for open networking include the Open Networking Foundation (ONF) and the Open Compute Project. The ONF is a non-profit industry-led group, which aims to leverage "network disaggregation, white box economics, open source software and software defined standards to revolutionize the carrier industry" (Open Networking Foundation, 2021[97]). The term "white box" typically is used to describe commodity, off-the-shelf hardware, which may not come with as many features and tends to be less expensive compared to purpose-built options (Nomios, 2023[98]). Off-the-shelf hardware running an open source operating system is easy to customise to meet specific business needs, given the many tools available for popular open source operating systems (e.g. Linux-based) (Nomios, 2023[98]). The Open Compute Project brings together a collaborative community to develop a fully open and disaggregated network technology stack. It has a module devoted to developing open and disaggregated networking hardware and software solutions and Linux-based networking operating systems, among others (Open Compute Project, 2021[99]). The Broadband Forum is another industry-led group with

synergies to the work being carried out under the other bodies. For instance, the Broadband Forum and the ONF are collaborating to help communication providers transition to become more open, automated and software-defined (Broadband Forum, 2019[100]).

Examples of open networking products include commercial offers to provide open networking software and infrastructure focused on the data centre, such as NVIDIA's offer leveraging a Linux-based network operating system (NOS) and Ethernet switches (NVIDIA, 2020[101]; NVIDIA, 2020[102]). The infrastructure enables open networking across software and infrastructure to maximise flexibility, including by allowing applications to be added onto hardware (Figure 2) (NVIDIA, 2020[102]). Dell is similarly offering open networking solutions for data centres, which leverage its open networking Ethernet switches (PowerSwitch) and the Software for Open Networking in the Cloud (SONiC) operating system, originally developed by Microsoft for cloud environments. Dell claims that its solution aims to automate much of the network configuration process, minimising errors and simplifying management and integration (Dell Technologies, 2021[103]). These offerings build upon the advancements to open up the chip market, for instance, the move from proprietary solutions to more open "merchant silicon" with the development of application specific integrated circuits (ASICs). ASICs are meant to be integrated into network systems, thereby supporting disaggregation in the network. ASICs play a key role in NVIDIA's open networking offer noted above; NVIDIA acquired Mellanox in 2020 and is leveraging Mellanox's Spectrum Ethernet switch ASIC in its offers (NVIDIA, 2020[101]).

Figure 2. Example of an open networking solution for a data centre proposed by NVIDIA



Source: NVIDIA (2020[102]), *Lenovo and NVIDIA spark new era of open networking,* https://blogs.nvidia.com/blog/2020/09/15/lenovo-open-networking/.

With open networking, networking hardware, such as switches, routers and firewalls, can be added onto existing hardware through open source applications, according to network needs (TechTarget, 2022[104]). Networking hardware, such as routers and firewalls, can also benefit from open source tools; for example, FRRouting is an open-source Internet protocol suite for routing (FRRouting, 2021[105]). Freedom of choice is a driving motivation of open networking, allowing operators to adopt network architecture that best fit their needs, across hardware, software, network operating system, and application (eWeek, 2020[106]). Openness also provides flexibility to program hardware based on specific needs or to meet evolving business demands, allowing customisation and giving more control over the network (eWeek, 2020[108]). This flexibility also gives networks the ability to scale up or down according to demands and also upgrade

network components without waiting for a proprietary upgrade. Other benefits may include economic efficiencies in total cost of ownership (TCO), with higher capabilities.

Open Radio Access Network (open RAN)

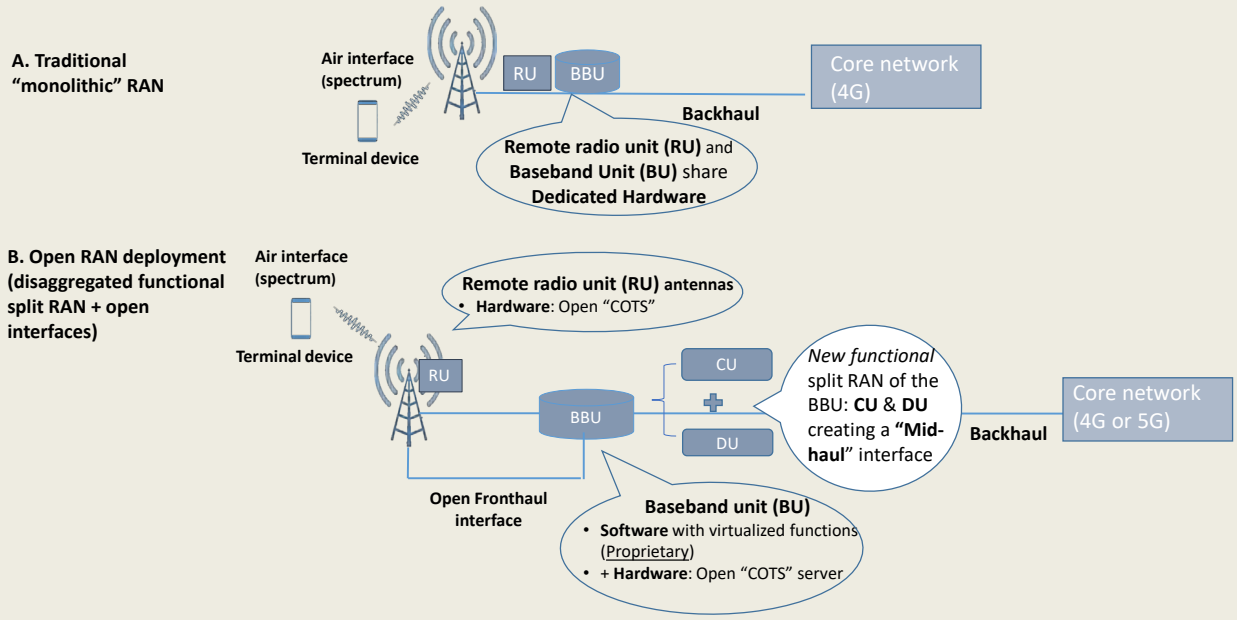
Recently, the trend to open and disaggregate networks has also been extending into the radio access network (RAN) of mobile networks. In previous generations of wireless networks, RAN architecture typically was "monolithic", served by a single vendor proprietary solution. With the disaggregation of the RAN, innovations leveraging virtualisation ("virtualised RAN") and/or open interfaces ("open RAN") have emerged that aim to give further flexibility and efficiency in networks.[15] Box 1 provides more details on the evolution towards an open RAN.

Box 1. From traditional RAN to open RAN

A monolithic base station in the past was made up of a Remote Radio Unit (RU) that is connected to a baseband unit (BBU) through a "fronthaul" interface. The BBU is composed of a Centralised Unit (CU) and a Distributed Unit (DU). The BBU contains digital modules that process signals from the RU and provides a communication interface to the core network, via backhaul. The RU is made up of antennas that receive and transmit wireless signals from the air interface (i.e., spectrum). Therefore, the BBU has both hardware and software elements, while the RU is composed of hardware. The 3GPP Release 15 disaggregated the baseband unit into a Centralised Unit (CU) and a Distributed Unit (DU), with a separate RU.

A virtualised RAN introduces virtualised network functions for the CU and the DU in the baseband unit, thereby decoupling hardware and software. However, the interfaces between RAN elements in vRAN architecture may be vendor-specific and therefore may not interoperate. With open RAN, the open, non-proprietary, and interoperable interfaces allow operators to select different vendors according to their needs. The figure below compares a traditional RAN deployment with an open RAN deployment, with a disaggregated functional split RAN from 5G 3GPP Release 15 and open interfaces, coupled with commercially available, off-the-shelf hardware (COTS).

Traditional "monolithic" base station compared to an open RAN deployment



Note: CU= Centralised Unit, DU= Distributed Unit, COTS= commercially available off the shelf equipment

Source: OECD based on Figures 9 and 10 of OECD (2022[23]), *Broadband Networks of the Future,* https://doi.org/10.1787/755e2d0c-en.

Sources: Ericsson (2023[107]), *Security considerations of Open RAN,* https://www.ericsson.com/en/security/security-considerations-of-open-ran; ETSI (2018[108]), *5G Release-15: NG-RAN Architecture description (3GPP TS 38.401 version 15.2.0 Release 15)*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3219; GSMA (2021[109]), Open and virtualised radio access networks: An explanatory guide, https://www.gsma.com/publicpolicy/wp-content/uploads/2021/02/GSMA_Open_and_Virtualised_Radio_Access_Networks_An_Explanatory_Guide_for_Policymakers.pdf; OECD (2022[23]), *Broadband Networks of the Future,* https://doi.org/10.1787/755e2d0c-en.

Open architectures have been promoted by industry-led bodies. The Telecom Infra Project, for example, was launched in 2016 to accelerate the development and deployment of open, disaggregated, and standards-based technology solutions (Telecom Infra Project, n.d.[110]; Telecom Infra Project, 2023[111]),. The O-RAN Alliance was established in 2018 to develop technical specifications for open RAN architecture (O-RAN Alliance, 2018[112]). Both of them signed an agreement in 2020 to work together to develop interoperable 5G RAN solutions (O-RAN Alliance, 2020[113]).

Open RAN architectures may incorporate some open source software components. For example, the O-RAN Alliance and the Linux Foundation are collaborating to develop open source software to implement O-RAN specifications, within the O-RAN Software Community (O-RAN Alliance, 2023[114]). However, open RAN software components may also include proprietary elements.

Implementing more open and interoperable network architecture can bring benefits as well as challenges, which are briefly presented below. The overall impact of open RAN architecture, considering both its benefits and challenges as well as the state of deployment, is a topic of much discussion. For example, a report from the EU NIS Cooperation Group notes “considerable uncertainty regarding scenarios of open RAN deployment in the short and medium term” (NIS Cooperation Group, 2022[115]). However, others point out that there is “intensive global activity across industry groups and companies to develop open RAN specifications and products” (DCMS, 2022[116]).

Open RAN architectures can bring several benefits. Some OECD members see the possibilities of open RAN to diversify the supply chain and allow for more new players to enter the market, drive competition and innovation in the RAN market segment, and ultimately lead to lower prices. Supply chain diversification could allow communication network operators to decrease or avoid depending on any one supplier, tying back to networks’ increasing criticality to economies and societies. Within industry, some stakeholders and, in particular, network operators view open RAN as a way to lower costs, decrease vendor lock-in and reliance on specific vendors, and align with domestic governmental priorities and/or requirements. They expect that open RAN architectures will reduce cost by allowing operators to choose commodity off-the-shelf options and open interfaces that allow disparate RAN elements to interoperate. Also, the disaggregation of the RAN gives operators the flexibility to place the DU, CU, and RU in different locations, according to their needs and plans to meet certain use cases (e.g., low latency cases).

However, Open RAN architecture could also bring some challenges in the area of competition. A report by the NIS Cooperation Group notes that while open RAN may encourage the entry of new players, there is a risk that “the market could also reconsolidate around a small number of suppliers, system integrators and cloud service/infrastructure providers, thus negating the diversification opportunity” , which “could lead to new critical dependencies in the mid- to long term” (2022[115]). That said, a thorough competition analysis, including definitions of the relevant market, would need to be undertaken to assess the level of competition across the communication infrastructure supply chain. At the same time, an open RAN architecture introduces additional complexity, which will require integration and testing, especially in the early stages of deployment and given the relative immaturity of the approach. Furthermore, it may reduce supplier

accountability in case of failures, given the larger possible number of responsible suppliers in an open RAN deployment.

Several providers of system integration (i.e. system integrators) have emerged to help operators address these challenges, including by managing the testing, integration, configuration, maintenance and ongoing support of the open RAN solution. This can include managing interactions with the various suppliers in the architecture to resolve issues. While service level agreements with individual suppliers will focus on the component level, a system integrator can assume responsibility to ensure the end-to-end solution upholds requirements in terms of quality and performance (NEC, 2021[117]). By extension, such an integrator could be charged with ensuring security standards are upheld by all its clients' suppliers. However, system integrators do represent a cost to deploy an open RAN network architecture. At this stage, the overall impact of system integrators on managing the complexity of open RAN deployment is a matter of debate. System integrators can have varying degrees of involvement and responsibility in the open RAN deployment. For instance, Fujitsu offers two models of support, with differences in terms of degree of involvement in the systems integration and the accountability for performance and ongoing maintenance (Fujitsu, 2020[118]). In addition, given the potential increased competition among suppliers in the open RAN environment, there may be more incentive to ensure accountability to their clients, in the face of lowered switching costs and decreased reliance on any one supplier.

Open RAN, in particular, is being actively discussed internationally and nationally in OECD countries. The Prague Proposals on Telecommunications Supplier Diversity put forward at the 2021 Prague 5G Security Conference, include a call for governments to support the open and multi-stakeholder development of technical standards to enable openness and interoperability, such as through open RAN technologies (National Cyber and Information Security Agency (NÚKIB), 2021[119]). The proposals have been supported by some OECD members, including the United Kingdom and the United States (DCMS, 2021[120]; White House, 2021[121]). Several OECD countries and partner economies are also considering open RAN in national initiatives, including Germany, the United Kingdom, the United States and Brazil, and others have engaged in partnerships which include the promotion of open RAN technologies, such as Australia, Japan, Korea and the United States (see Annex 2. Open RAN initiatives in OECD countries for further details).

Among industry, several initiatives aim to develop the open RAN ecosystem. Telecom Italia (TIM) signed a Memorandum of Understanding (MoU) with other European operators (Deutsche Telekom AG, Orange S.A., Telefónica S.A. and Vodafone Group Plc) to promote, develop and implement open RAN technology in Europe (TIM, 2021[122]). The group jointly published a report in November 2021 calling on European governmental and industrial stakeholders to "urgently prioritise" open RAN through five specific policy recommendations (Telefónica, 2021[123]). Simultaneously, operators are conducting trials and testing of open RAN architecture and some industrial stakeholders have established research and development (R&D) centres to development technologies needed to support open RAN deployments.

The actual roll-out of open RAN deployments is at an early stage and is still taking shape. However, some operators have moved from the testing phase to actual live deployments or have plans underway. In 2020, NTT DOCOMO, one of Japan's MNOs, adopted open interfaces for 4G, and successfully deployed the network. In the same year, Rakuten Mobile entered the Japanese market and was the first to deploy an "open, virtualised, distributed radio access network" for its 4G "greenfield" network (i.e. establishing a network where none had existed before, as opposed to building on top of legacy networks) (Rakuten Mobile, 2020[124]). In February 2022, Rakuten's virtualised cloud-native open RAN network reached 96% coverage of Japan's population (Rakuten, 2022[125]). In June 2021, Deutsche Telekom announced its live deployment of open RAN in Neubrandenburg, with a multi-vendor architecture including Dell, Fujitsu, Intel, Mavenir, NEC and Supermicro (Deutsche Telekom, 2021[126]). 1&1 AG, together with Rakuten Group, Inc., and DISH Network with Dell Technologies, both announced plans for open RAN deployments (Rakuten, 2021[127]; DISH Network Corporation, 2021[128]). These are only a few examples of industry actions related to open RAN; further examples on trials, testing, R&D centres, and deployments can be found in Annex 2. Open RAN initiatives in OECD countries.

While many in industry see potential benefits in open RAN, some hurdles remain. For example, some industry players have argued that greenfield open RAN deployments pose fewer challenges than deploying the technology on existing networks (T-Mobile USA, 2021[129]). To note, the open RAN deployments of Rakuten Mobile, 1&1 and Dish are examples of greenfield networks, while Deutsche Telekom has a legacy network.[16] Other stakeholders, while supportive of open RAN, also recognise the challenges to maintain network reliability and performance when transitioning to open architectures (AT&T Services, Inc., 2021[130]).

Security implications

Increased openness can bring both possible benefits and challenges. Prior to discussing them, it is important to highlight the following considerations.

First, **open architectures, such as open RAN, are not inherently more or less secure than traditional network architectures**. In general, the level of digital security of an architecture model depends on several factors, many of which are not strictly specific to the model, such as the implementation context, which can vary over time (e.g. changing threats) and space (e.g. applicable law). As always in digital security, the overall balance between security benefits and challenges of a particular model needs to be considered in context, as part of a generally broader risk assessment. This means that many of the possible high-level security benefits and challenges from increased openness described below are not automatic, nor systematic. They will rather depend upon many factors and may sometimes be mitigated (for challenges) or optimised (for benefits). Additionally, for the challenges in particular, some of these security considerations may be applicable to other network architectures and not unique to open RAN (NSA/CISA, 2022[131]; FCC CSRIC VIII, 2022[132]; Quad Critical and Emerging Technology Working Group, 2023[133]).

Second, **the various aspects of the trend towards more openness are not necessarily interlinked**. For instance, the modularisation of networks does not necessarily entail the use of open source software. The development of open architectures could also result in operators using a mix of open and proprietary software. Similarly, integrated suppliers of communication equipment, which provide a more traditional network architecture, often integrate open source components in their offer.

Third, as **the effective deployment of more open architectures is relatively new,** it is difficult to gather sufficient empirical evidence and assess the long-term impact of this evolution on the digital security of communication networks at the time of writing. In the case of mobile networks, for instance, open RAN is still emerging and will likely co-exist alongside traditional RAN implementations for a significant period, which makes it challenging to analyse its impact on digital security in isolation (NIS Cooperation Group, 2022[115]).

In addition, **the pace and level of uptake of more open architectures by the industry in the short and medium term is uncertain**, including for open RAN. As discussed above, different scenarios may occur, ranging from a relatively low adoption limited to some market players to a very significant uptake by most operators across OECD countries. While increasing competition and reducing costs are often acknowledged as the main drivers of the development of open RAN, enhancing digital security appears to be a less prominent factor for industry, at least in the early stages of open RAN adoption, even though it may evolve.

Fourth, **the deployment of open architectures is likely to result in a shift of digital security risk, however its overall effect on the risk level on the longer term is unknown.** Whether this shift will result in higher or lower risk in the medium to long term will depend in part on how stakeholders will handle it and how threat actors will adapt to it. It is essential to recognise and understand this shift to make appropriate risk management decisions at the operational (e.g. design and implementation of open architectures) and public policy levels.

Security benefits

The evolution towards more openness may bring a number of benefits for digital security risk management in communication networks. First, the trend towards more openness is enabling a **diversification of the supply chain** of communication networks, which is likely to **reduce network operators' dependency** on a relatively small number of suppliers. This could limit the emergence of single points of failure and reduce systemic risk, which has been identified by many stakeholders as a key security challenge for communication networks (ENISA, 2019[36]). In fact, supply-chain dependencies often lead to closed technical "monocultures" prone to systemic risk by increasing the likelihood that a single vulnerability creates a widespread outage simultaneously affecting many operators, causing cascading failures on other critical activities whose functioning relies on communication networks (OECD, 2019[134]).

Second, as more open architectures are expected to enable **more competition** in the supply chain of communication networks, they may also **stimulate innovation**, including to develop new tools for digital security risk management. In fact, lower barriers to entry would likely result in a wider range of suppliers, which could use digital security as a market differentiator. Reduced switching costs, resulting from the interoperability enabled by open interfaces, could also further incentivise vendors to be more responsive to digital security risk, for instance regarding effective and timely vulnerability treatment and responsible end-of-life (EOL) policies (OECD, 2021[135]). "White box" equipment could also facilitate the development of the market for specialist security firms (e.g. managed service providers) focusing on communication networks, if operators have appropriate incentives to invest in digital security.

Another key potential security benefit of openness is the **positive evolution towards more transparency**, away from "security by obscurity". More open architectures enable operators and digital security services providers to have more in-depth visibility and understanding of network architectures and equipment, to perform more comprehensive vulnerability scanning and management, to monitor data flows and to detect threats and abnormal traffic patterns at a deeper level (Deutsche Telekom, Orange, Telecom Italia, Telefónica, Vodafone, 2021[136]). In addition, the increased use of open source software – which is also present in traditional network architectures – could also facilitate code review and security auditing of associated products.

In the case of mobile networks in particular, open RAN provides a good illustration of these potential benefits, under certain conditions. In particular, the development of open RAN could:

- Enable supply-chain diversification, which would reduce risks related to dependency on a few suppliers at the RAN level.
- Increase interoperability between suppliers and competition at the RAN level, thus providing network operators with more choice for their equipment and reduced switching costs. Operators could then use security as a factor when choosing their suppliers, alongside other factors such as performance, price and usability, to name a few.
- Allow operators to better tailor security to their needs and use cases, through greater modularity and flexibility.
- Foster the emergence of an ecosystem of partners with a mutual interest to share security-related information more readily, which could hasten mitigation actions.
- Facilitate faster roll-out of security updates, innovations and best practices by reducing technical lock-in.
- Increase the ability to detect and address security issues at the network edges, thanks to the facilitated collection of RAN-level security information.
- Empower operators to replace physical or digital elements more easily, thanks to a combination of lower interdependence between hardware and software and greater modularity of network components.

- Increase transparency for both communication networks and their supply chain. A more open network architecture through open RAN can increase the transparency in network management and can make it easier to detect risky or faulty components.

Security challenges

The evolution towards more openness may also bring a number of challenges for digital security risk management in communication networks. First, it is often emphasised that complexity is “the enemy of security" (Schneier, 1999[137]) and the diversification of suppliers as well as the development of multiple open interfaces in communication networks are likely to **increase the complexity of network architectures** (NIS Cooperation Group, 2022[115]). As a result, the integration of many network modules from various suppliers and the multiplication of open interfaces in open RAN environments increases the risk of misconfigurations. In addition, more third-party applications that connect to open RAN nodes can **expand the attack surface** and provide malicious actors with new opportunities to exploit vulnerabilities. More open APIs may raise security considerations as third-party applications can access data and information flows (NIS Cooperation Group, 2022[115]). Lastly, the decoupling of software and hardware resulting from a virtual RAN (Box 1) would require an end-to-end chain of trust, which may prove difficult to establish and maintain, as hardware, operating systems, and application software can come from different vendors.

Second, open architectures may **make digital security risk assessment and mitigation more difficult.** Network operators would need to assess digital security risk from a larger number of suppliers, from various combinations of equipment, and to perform reassessments regularly as suppliers’ risk profiles can quickly evolve. Security audits may become more challenging in open architectures, as digital security risk assessment and treatment would need to encompass a combination of vendors and integrators, rather than focusing on a single vendor. Furthermore, since these different components will be interconnected, a vulnerable component may impact the security of the overall network. The need to trust a larger number of interoperable products may also weaken the chain of trust between software and hardware equipment. These considerations are relevant to all open architectures, including in open RAN environments.

Third, as open architectures, such as open RAN, introduce many more vendors into the mobile network supply chain, they may result in **responsibility gaps** for digital security risk management between network operators, equipment manufacturers, software vendors and service providers. Defining responsibilities along the supply chain is a common challenge across the ICT ecosystem. Therefore, network operators will need to carefully examine each potential responsibility gap with their suppliers, including in an open RAN environment, as the latter may have different policies regarding digital security risk management responsibility allocation.

Furthermore, the potential positive effects on digital security from increased competition in the supply chain are not automatic. To be effective, they would require stakeholders to value digital security appropriately, compared to other economic factors such as time-to-market, cost-effectiveness or usability. Depending on the context, such trade-offs may not be optimal and may call for additional incentives (e.g. certification or legal requirements), in particular in case of externalities and information asymmetries. Market forces alone are rarely sufficient to encourage market players to invest in digital security, particularly in the early stages of emerging technologies during which usability, cost-effectiveness and “go-to-market” strategies are often prioritized (OECD, 2021[8]).

When security is not included in the design of a technology at the beginning (i.e. “security-by-design”) but rather added later on, it may take decades of incidents for stakeholders to develop and implement effective security mechanisms. The consumer IoT market is one of the most recent illustrations of such misaligned market incentives. However, Business-to-Business (B2B) markets, such as those where communication network operators are clients of suppliers (e.g. equipment, cloud), may be less prone to information asymmetries than Business-to-Consumers (B2C) markets. In fact, it may be argued that large businesses

are more likely to benefit from financial resources and expertise in digital security, and from a more significant bargaining power, which may further enable increased competition to deliver enhanced digital security.

Implementing a security-by-design approach is also important at the technical specifications level, both for mobile networks generally, and open RAN specifically. However, some governments caution that the specifications being developed for open RAN at the O-RAN Alliance may not include security from the outset of the development process (NIS Cooperation Group, 2022[115]). For example, a recent risk analysis of open RAN commissioned by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik (BSI)) asserted that the current development process to define O-RAN specifications was not following a "security/privacy by design/default" approach (BSI, 2022[138]). Further, the findings of the risk assessment found "medium to high" security risks arising from several of the interfaces and components in the O-RAN specifications (BSI, 2022[138]). The O-RAN Alliance's Security Focus Group (SFG), which is tasked with developing security specifications, announced the second version of its security requirements specifications in April 2022 (O-RAN Alliance, 2022[139]). Making these security requirements specifications and related risk assessment information publicly available and opening the developments of these specifications to interested stakeholders would be beneficial to address security challenges.

There is also a **debate about the openness and transparency of the organisations in charge of developing standards related to open network architectures**, in particular in comparison to Standard Development Organisations (SDOs) such as ETSI, 3GPP or similar structures such as the IETF. These structures typically develop standards following principles such as transparency, openness, inclusiveness, impartiality, and consensus. Some government stakeholders have raised questions regarding the application of these principles by *ad-hoc* organisations developing specifications on open RAN, such as the O-RAN Alliance, in particular regarding the important decision rights held by the Board, which represents a subset of total members and is composed of mobile network operators only (NIS Cooperation Group, 2022[115]). They have also pointed out that deficiencies in the O-RAN technical specifications development process may lead to insecure RAN products (NIS Cooperation Group, 2022[115]). The O-RAN Alliance has made efforts to increase transparency and inclusiveness. For instance, ETSI has recently released a specification developed by the O-RAN Alliance, following its formal review process by ETSI experts (ETSI, 2022[140]). The O-RAN Alliance plans to submit further specifications to ETSI to be recognised as ETSI specifications. However, the O-RAN Alliance could further increase transparency and inclusiveness in their overall decision-making process as well as access to their work.

In parallel to but distinct from open RAN, **the increased use of open source software**, in both open and closed network architectures, **may bring new challenges for digital security risk management** in communication networks. While the use of open source software increases transparency and allows for more code review, it does not necessarily entail a higher level of digital security, especially if there is a lack of community support to provide digital security expertise and contribute to code security maintenance (OECD, 2021[135]). As some open source components can be reused in a very large number of diverse applications, including proprietary products, they can be viewed as a source of systemic risk. Furthermore, open source software projects may suffer from a lack of resources for digital security, such as for carrying out security audits and bug bounties. Initiatives from governments and other stakeholders to mitigate this risk are underway, as further discussed below.

Artificial Intelligence (AI) in communication networks

AI is expected to play an increasing role in communication networks

AI has been lauded for its potential to increase efficiency across the economy, not just communication. AI has a broad array of use cases, touching many critical sectors in society. Prior work at the OECD defines

an AI system as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments" (OECD, 2019[141]). However, for the purposes of this report, only AI's role within communication networks will be considered, rather than the broader topic of AI more generally or the AI use cases benefitting from high-speed, high-quality connectivity.

Operators are considering how to use new forms of machine learning and automation to better manage and operate their communication networks. The use of AI systems in communication networks can help operators improve network management and operation, aid in incident prevention, predict maintenance for hardware and facilitate the analysis of customer behaviour and demand. AI's current role in communication networks lies primarily in monitoring performance, predicting maintenance, and optimising specific parameters, such as spectrum, quality of transmission, and routing (Dialogic innovation & interaction, 2020[142]).

Communication networks have already begun leveraging AI and machine learning (ML), specifically for automation of network management. For example, Finnish operator Elisa has been developing different automation levels in its networks for the past decade; it now offers automation solutions leveraging AI/ML for network operation and optimisation to interested operators via a spin-off company called, "Elisa Automate" (Elisa Automate, 2020[143]). Vodafone and Telefonica have also developed AI/ML tools to facilitate interactions with customers, including customer support (Vodafone, 2023[144]); (Telefonica, 2021[145]). In Korea, communication service providers have also ventured to use AI systems to improve network management. SKT developed an AI solution called "Tango", or "Telco Advanced Next-Generation Operations Support System" that provides data analytics and optimised automation based on AI technology in real-time, thereby reducing the cost associated with network management tools. SKT expects that Tango will lead to a 40% cost reduction after five years compared to the total cost of operating legacy operation support systems (GSMA, 2019[146]). Another example in the country is KT's "Dr. Lauren", which is an AI-based network failure Root Cause Analysis solution, commercialised by KT in November 2018. It collects operational data generated from the network and performs AI-based data analysis to identify the root cause of network failures (GSMA, 2019[147]). KT estimates operating expenses (OPEX) savings of USD 1.2 million annually due to Dr. Lauren, through intelligent remote monitoring and minimising failure recovery time (GSMA, 2019[147]).

With a similar aim to KT's Dr. Lauren, Vodafone and Nokia announced an "Anomaly Detection Service" based on ML that can detect mobile network anomalies quickly and act to correct them before impacting Vodafone's customers (Vodafone, 2021[148]). The service will run on the Google Cloud and will stream data to Vodafone's analytics platform from various points across the multi-vendor environment. This allows data to be pooled and analysed to detect patterns and identify anomalies (OECD, 2022[23]). The anomaly detection service is offered as a service on Nokia's Cloud and Network services (Vodafone, 2021[148]).

5G networks are expected to benefit from AI systems. AI can help improve overall network performance and reliability, simplify network management linked to network slicing, optimise network capacity and handle vast amounts of data. As networks begin to integrate more aspects of openness, including for open RAN, for instance, AI can help operators manage complex network architectures. According to the O-RAN Alliance, "O-RAN architecture is the foundation for building the virtualised RAN on open hardware and cloud, with embedded AI-powered radio control" (O-RAN Alliance, 2020[149]). Open RAN architecture may improve the flexibility and agility of the network by RAN automation, which may include the use of AI and machine learning for network optimisation (O-RAN Alliance, 2020[150]). In addition, AI may support equipment vendors and operators to reduce energy consumptions costs of networks by finding new ways of making networks more energy efficient without impacting network performance. As one example, Ericsson ran a trial to use AI and machine learning (ML) in network management and automate MIMO energy management in cell sites in Vodafone's network in Portugal (Ericsson, 2019[151]).

AI systems may also have linkages with edge computing, in which AI applications and services may be embedded at the edge, leveraging the architecture of edge computing that moves computing and processing resources to the edge, closer to the end user. The European Commission granted funds to research this under the Horizon 2020 call for proposals on the topic of "a secure and reusable Artificial Intelligence platform for edge computing in beyond 5G networks" (European Commission, 2021[152]). Looking beyond 5G, industry experts have begun to discuss the development of 6G networks. While still in the early stage of discussions, 6G is expected to rely on AI and ML capabilities, namely big data analytics, closed loop network optimisation and intelligent wireless communication (Siriwardhana et al., 2021[153]).

Security implications

Security benefits

The use of AI in communication infrastructure holds a significant potential to improve digital security risk management, in particular in light of the other trends described above, which are likely to increase the complexity of communication networks and their supply chain.

First, **AI-enabled digital security systems can automate the detection of malware and identify patterns of suspicious behaviour and traffic**. In that respect, these systems can be faster and more effective than traditional approaches. AI can assist stretched and overworked digital security teams, which is especially useful given the shortage of skilled digital security professionals. Furthermore, AI can automate certain digital security tasks such as vulnerability scanning, addressing common threats, monitoring high volumes of data, and alerting for sophisticated suspicious events. This enables staff to allocate human expertise more effectively. Automation can also decrease the likelihood of human errors such as misconfigurations and negligence (OECD, 2020[154]).

In addition, **the use of AI by communication infrastructure suppliers has the potential to increase the level of digital security of key products** such as core network and RAN equipment, as well as services such as cloud and network management. These suppliers could use AI systems to enhance the "security-by-design" of their products (OECD, 2021[8]), in particular to complement approaches such as DevSecOps (Development Security Operations), for instance to detect and address emerging vulnerabilities before products are commercialised.

Furthermore, the use of AI could significantly facilitate and accelerate the adoption of zero-trust security models, which provide enhanced security risk management by moving away from traditional perimeter-bound security practices, and could significantly enhance the ability of stakeholders to manage digital security risk in the context of the increasing complexity of communication networks and of their supply chain. Zero-trust is further discussed below.

Security challenges

However, the use of AI in communication networks could also result in new challenges for digital security risk management. First, AI systems that are not understandable nor transparent can create significant challenges for digital security risk management. In general, it can be difficult to understand how an AI-based decision was formed, to audit its logic and ensure that there are no errors or flaws in the system. For example, an AI system could detect traffic related to the use of a new protocol as abnormal and block it by mistake. The relative opacity of how some AI systems make decisions can raise responsibility, accountability and trust issues. If a breach of availability happens because of an AI-based decision, it may be difficult to attribute responsibility among the various participants in the AI system (Dialogic innovation & interaction, 2020[142]). This potential lack of transparency and difficulty to understand AI systems may raise questions regarding the ethics of such systems, in particular if those systems are built and maintained by dominant market players in other segments, such as network equipment or cloud services. In such

conditions, AI systems could be biased, e.g. to favour the performance of the equipment belonging to the same conglomerate or to deteriorate the quality of service of competitors' equipment.

In addition, malicious actors may use AI to develop new exploits (i.e. attack techniques), discover new vulnerabilities and bypass traditional security measures. The perspective of an "arms race" between defenders and attackers in the use of AI is probable, in particular regarding sophisticated, state-sponsored threat actors that may benefit from significant resources, including for R&D.

Finally, because the functioning of AI extensively relies on the collection and processing of data, the development of AI-enabled systems is likely to enable a new category of cyberattacks based on data poisoning, including inserting or manipulating data or logic corruption (Siriwardhana et al., 2021[153]). Such attacks would not target the communication infrastructure directly, but rather the data processed by the AI-enabled system. In that perspective, data poisoning attacks could be considered as a new category of "supply chain" attacks. Such attacks could also breach the confidentiality of algorithms to exploit possible weaknesses (Dialogic innovation & interaction, 2020[142]). Security risk related to AI systems could propagate throughout an operator's network if its AI systems are interlinked.

Cross-cutting overview of security implications

The different trends mentioned above have implications on the security of networks, which can be broken down into i) the main benefits for operators, and ii) the high-level challenges that need to be addressed to successfully enhance the digital security of communication networks.

The technological evolution towards increased virtualisation, the use of cloud services and a move towards openness bring significant changes to the design, deployment and management of communication networks. This evolution represents a major shift from communication networks of the 20th century, which were more hardware-based, and where network management and other critical functions were essentially located in core network equipment.

Main security benefits: a potential for increased transparency, automation and supply chain diversification

The virtualisation, increased integration of cloud services and increased openness of networks can bring significant benefits for digital security risk management. They are likely to facilitate vulnerability scanning, enable more visibility on the network (e.g. identification of assets, detection of potential threats), a higher level of automation of security controls, more efficient use and allocation of security resources (e.g. deployment of security updates, filtering) and better network segmentation. These benefits could facilitate moving away from perimeter-bound security practices towards security approaches that presume the presence of intruders in the network (see a discussion of "zero trust" below).

Similarly, the potential to slice 5G networks can enable operators to better isolate their clients' Internet traffic and related data, contain potential incidents more effectively and better allocate security resources. The increased role of important cloud providers and system integrators could enable communication networks to benefit from these organisations' significant capabilities in managing digital security risk.

The emerging applications of AI in communication networks hold the promise of extending those benefits even further. AI-enabled digital security systems can automate the detection of malware and identify patterns of suspicious behaviour and traffic rapidly. Faster detection and mitigation can bring significant benefits for risk management. In addition, the use of AI by communication infrastructure suppliers has the potential to increase the level of digital security of key products, such as core network and RAN equipment, as well as cloud and network management services.

The momentum towards an increased openness of communication networks can also bring significant benefits to digital security risk management. Open architectures such as open RAN can diversify the communication infrastructure supply chain and help reduce dependency on a few suppliers, which would decrease systemic risk. The commoditisation of network equipment and the increased modularity of network architecture also have the potential to spur innovation and competition in the communication infrastructure supply chain. Increased competition may enable both demand-side and supply-side actors to better value digital security, for instance by allowing suppliers to use digital security as a market differentiator[17] (OECD, 2021[135]). The development of "white box" products, as embodied in the dynamics toward open RAN, can enable operators to benefit from increased visibility on their network architecture, equipment and traffic. Such increased visibility may enable better network monitoring, as well as more effective threat detection and mitigation.

High-level challenges: a shift in scale, scope and speed

However, virtualisation, the use of cloud services, the movement towards more openness and the increased criticality of networks also bring significant challenges to managing digital security risk in communication infrastructure. In particular, they result in an expanding attack surface, a broader and more complex supply chain and an aggravating threat landscape.

An expanding attack surface

The scale of communication networks' attack surface (i.e. the set of points of an information system that are potentially vulnerable to an attack) **is expanding to an unprecedented level**. Communication networks are becoming more interconnected and their architecture increasingly complex. Because they are increasingly software-defined, cloud-based and virtualised, communication networks contain more software vulnerabilities that can be exploited remotely and can be more difficult to manage, especially for organisations that lack a skilled workforce, such as smaller operators. These dynamics also contribute to a higher risk of misconfigurations, a key source of vulnerabilities for organisations, including for those relying on cloud services (OECD, 2021[135]). In addition, communication networks are now built as an overlay of multiple logical and physical layers and involve an increasingly diverse set of user categories, including M2M traffic and IoT devices. Managing trust, identity and authentication across such a complex context is a significant challenge for network operators. Beyond digital security attacks, this increasing complexity also allows for more system failures due to unintentional incidents such as human errors or updates that result in the unavailability of the network.

In addition, it is becoming increasingly difficult for network operators to manage the security lifecycle of the products they rely on. Software-defined and cloud-based networks typically rely on products whose security lifecycle is considerably shortened compared to previous generations of networks, i.e. for which security updates may need to be rolled-out on a weekly basis and that may reach their end-of-life (EOL), i.e. end of security support, after only a few years (OECD, 2021[135]). While the use of "security-by-design" methodologies by suppliers may reduce the number of vulnerabilities contained in the products used in communication networks, it will not prevent the need for operators and their suppliers to adopt more dynamic vulnerability treatment policies and to effectively manage the EOL of their products. In fact, while much of the public debate around vulnerabilities focuses on "zero-day" vulnerabilities (i.e. which are unknown to the party able to fix them), the vast majority of successful digital security attacks rely on known vulnerabilities that have not been patched yet, either because of poor patch management processes or because they pertain to products that have reached their EOL and are no longer supported (OECD, 2021[8]; OECD, 2021[14]).

An example of the increasing scale of the attack surface is the difficult management of digital security risk in so-called "brownfield" networks spanning different mobile network generations. In fact, in most cases, a new generation of network is deployed over a pre-existing network and coexists with it for a transition

period. These "brownfield" networks differ from "greenfield" networks, i.e. where no mobile communication networks were previously deployed. While much of the public debate focuses on the impact of emerging technologies on the digital security of communication networks, legacy network vulnerabilities can also have a significant impact as overlay networks typically coexist (see Box 2).

Box 2. The SS7 vulnerability – how legacy protocols can affect the digital security of communication networks on the road towards 5G

In most instances, 5G coexists with older generations of wireless networks such as 2G, 3G and 4G technologies. Currently, most 5G networks are non-standalone 5G networks, using 4G core networks. Different generations of networks will function in parallel during a transition period, which could last from a few years to a few decades. The deployment of Internet of Things (IoT) devices with low network requirements (e.g. in terms of latency or bandwidth) could extend the usage of 2G or 3G networks, as these devices may run on those legacy networks.

The co-existence of different generations of networks makes them vulnerable to flaws inherited from legacy protocols. Developed in the 1970s and largely adopted since, SS7 (Common Channel Signaling System 7) is a set of protocols governing the exchange of signaling messages, including setting up and terminating telephone calls over Public Switched Telephone Network (PSTN). This protocol is still widely used in 2G and 3G networks today.

SS7 was developed when only fixed-line operators had access to networks, which made digital security less of a concern. In today's communication networks, SS7 is no longer isolated and can be accessed by both legitimate operators and malicious actors. Furthermore, it contains architectural flaws that make it vulnerable to a range of attacks, enabling malicious actors to easily listen in on calls, intercept SMS messages, and instigate various forms of fraud (i.e. by simply downloading a software largely available online).

The example of SS7 shows how traditional vulnerabilities continue to be present in communication networks and exploitable by malicious actors, even though the public debate tends to focus on vulnerabilities related to 5G technologies. Policy makers should therefore encourage stakeholders, in particular network operators, to adopt a holistic approach to digital security, grounded in risk management and taking into account the complexity of overlay networks.

Source: FirstPoint (2020[155]), *A Step by Step Guide to SS7 Attacks*, https://www.firstpoint-mg.com/blog/ss7-attack-guide; Positive Technologies (2018[156]), *SS7 vulnerabilities and attack exposure report*, https://www.gsma.com/membership/wp-content/uploads/2018/07/SS7_Vulnerability_2017_A4.ENG_.0003.03.pdf.

A broader and more complex supply chain

In addition to this expanding attack surface (scale), **the supply chain of communication networks' operators is getting broader and more complex**, leading to a change of scope for managing digital security. The technological advancements described above tend to increase the dependency of network operators on some of their suppliers and to redistribute control and responsibility for the management of digital security risk along the entire value chain. In particular, network operators can increasingly be dependent on four categories of suppliers (introduced above):

- Suppliers of communication hardware equipment;
- Managed service providers (MSPs).
- Cloud service providers; and

- System integrators.

5G technologies, in particular, have begun to demonstrate the increased role of these suppliers in building and operating networks, the complexity of the interlinkages between suppliers and operators and the degree of dependency on individual suppliers (NIS Cooperation Group (EU), 2020[18]).

More broadly, **the supply chains of the products and services commonly used in communication networks are often complex**, which makes the allocation of responsibility in case of a digital security incident even more difficult (OECD, 2021[8]). The SolarWinds incident demonstrated the widespread impact that a breach of one MSP could have on a large number of organisations, as around 18 000 of SolarWinds' customers were infected by malware through a software upgrade of its Orion product, including government agencies (SolarWinds Corp., 2020[93]). In another "supply chain" incident, Microsoft reported zero-day vulnerabilities in Outlook Exchange Servers, with estimates of over 400 000 servers being initially vulnerable (Microsoft, 2021[157]). The extent of this vulnerability across organisations and within federal agencies prompted the US Cybersecurity and Infrastructure Security Agency (CISA) to issue an emergency directive to mitigate the vulnerabilities (CISA, 2021[158]). Communication network operators, like any other organisation, are also vulnerable to supply chain vulnerabilities.

The evolution towards more openness in networks (e.g. open RAN), and more specifically the modularisation of network architecture and commoditisation of communication equipment, is likely to bring more transparency. At the same time, it can aggravate the complexity of communication networks' supply chains, as network operators will typically need to manage the vulnerabilities associated with the products and services of several suppliers. The need for the skills and expertise of third parties such as cloud providers, system integrators and MSPs may therefore increase, as they could become instrumental to manage the growing complexity of network architecture and of their supply chain. However, this could also increase the number of actors benefiting from privileged access to communication networks, which may blur the allocation of responsibility and create liability challenges, lead to possible gaps in digital security risk management and result in a higher systemic risk of supply chain attacks.

An aggravating threat landscape

Lastly, managing the digital security of communication networks entails coping with a constantly evolving threat landscape. As communication networks become increasingly critical, malicious actors' appetite to breach their availability, integrity or confidentiality is significantly increasing (NIS Cooperation Group, 2019[38]). The aggravation of the threat landscape is further enabled by two distinct trends that are not specific to communication networks but affect digital security overall. First, the commoditisation of exploits enables a number of new entrants to aggressively target operators of critical activities, in particular through availability attacks (e.g. DDOS or ransomware "as-a-service"). Such new entrants include criminal organisations as well as hacktivists (i.e. individuals or organisations that launch cyberattacks for ideological purposes). Second, there is an increasing sophistication of State-sponsored threat actors (APTs), which are able to stealthily breach the confidentiality of communication networks and carry out attacks on their availability as suggested by recent research (NIS Cooperation Group (EU), 2020[18]). Lastly, it is likely that increased geopolitical tensions result in more aggressive cyberattacks targeting critical activities, including network operators and their suppliers.

Overall, this shift in scale, scope and speed makes communication networks and the management of their digital security risk a more complex challenge than in previous decades and makes it more difficult for network operators, in particular smaller ones, to effectively manage digital security risk. It also increases the role of third parties such as equipment suppliers, cloud providers, integrators, software producers and managed service providers.

Policy discussion

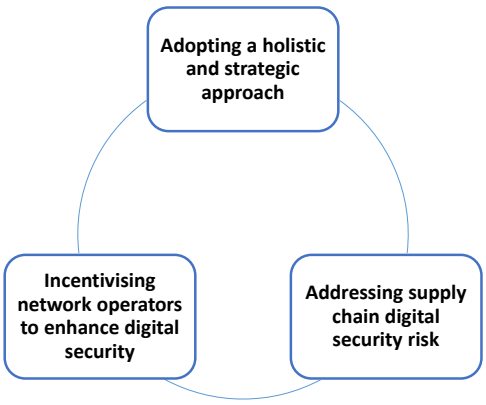
To address the cross-cutting challenges outlined above, policy makers should consider ways to support an enabling environment that encourages stakeholders to reach an optimal level of digital security. When undertaking policy initiatives, governments and regulators have to first establish policy objectives, which will guide the specific policy actions that can be tailored to meet the challenges.

Policy objectives

Because of the high-level challenges outlined above, current policy frameworks applicable to the digital security of the communications sector may be insufficient and may need to be complemented, for instance considering upcoming mobile network generations (NIS Cooperation Group (EU), 2020[18]). In fact, enhancing the digital security of communication networks is too often considered to be a technical issue that requires primarily technical remedies, whereas economic factors also play an important role, as market incentives on their own are unlikely to fix gaps in digital security risk management (OECD, 2021[91]).

To create an enabling policy environment that incentivises stakeholders to address security challenges, overall policy objectives can be broken down in three key areas or building blocks: i) adopting a holistic approach to digital security risk management in communication networks; ii) incentivising network operators to enhance digital security, and iii) addressing supply chain digital security risk (Figure 3). These building blocks are interdependent, and their effects are cumulative.

Figure 3. Three policy objectives to enhance the digital security of communication networks



Source: OECD.

Adopting a holistic and strategic approach

To manage the increasing complexity of networks and the evolving market dynamics described above, there is a need for governments to adopt a holistic and strategic approach towards enhancing the digital security of communication infrastructure. Such a holistic approach should i) consider the entire lifecycle of products and services on which operators rely, ii) gather all relevant stakeholders and iii) be co-ordinated across the whole government and at the international level. To facilitate their implementation, governments can insert these objectives in their broader national digital or cyber security strategy.

While much of the public debate regarding the digital security of communication networks focuses on the design of communication equipment, vulnerabilities may arise at any stage of the communication equipment's lifecycle, as shown in Figure 4. These vulnerabilities include i) poorly designed standards, in which case they are likely to affect most products that implement the standard; ii) product development

that does not implement security-by-design principles and practices; iii) a misconfiguration or a faulty deployment of products; or iv) an operational flaw, for instance an incomplete patch management by the operator. At each step, different stakeholders are involved in digital security risk management.

Figure 4. Architecture of communication networks: a lifecycle approach

Source: Ericsson (2023[159]), *Telecom Security*, https://www.ericsson.com/en/security.

Government initiatives must take into account the entire lifecycle, from the development of standards to the deployment and operation of communication equipment. Each step shown in Figure 4 involves different stakeholders, which share responsibilities for managing digital security risk throughout the product lifecycle. Given the increasing complexity of communication networks' supply chain and lifecycle, no single stakeholder can be held entirely responsible for enhancing overall digital security. Thus, when governments design policies to enhance the digital security of communication networks, they need to consider the following four categories of stakeholders, which have a specific role in digital security risk management:

- Communication network operators;
- Users, including industrial users such as operators of other critical activities;
- Suppliers of products and services, including communication hardware equipment and software, system integration, managed services and cloud services;
- Standard Development Organisations (SDOs).

Designing policies that apply to the first two categories of stakeholders is often within the remit of governments. On the other hand, suppliers form a complex ecosystem of firms of variable sizes, often headquartered outside national borders, which are more difficult for public authorities to oversee. As a result, it is more difficult for governments to ensure that all groups of suppliers assume their specific responsibility or "duty of care" to manage the digital security risk associated with their products and services (OECD, 2021[8]), a topic further discussed below. Regarding the last category of stakeholders, SDOs, governments can support the development of standards that provide a sufficient level of digital security from their perspective by participating in standard development processes and ensuring that their governance meets the principles of openness, transparency, consensus-driven discussion, inclusion and multi-stakeholderism, as discussed below.

A holistic approach also includes co-ordination across different governmental agencies, such as the government department in charge of communication policy; communication regulator; digital security regulator; competition authority; department in charge of economic development; etc. A clear definition of responsibility and/or mandates between the different bodies is also essential. Some countries may centralise responsibility for digital security in one organisation across sectors, whereas others may give the sectoral regulator responsibility for defining and supervising digital security policies of the sector under its remit, with the support of a more specialised, sector-neutral cybersecurity agency (Bernat, 2021[160]). Regardless of the approach, collaboration is essential to leverage the respective expertise of each agency. Digital security legislation may be sector-specific, or it could address the security of the communication sector as part of a larger horizontal security framework, for instance on protecting critical infrastructure. Managing overlaps in legislation and regulatory remit is a critical piece to establish an enabling environment to enhance digital security, providing clarity for both industrial and governmental stakeholders.

Lastly, such policies are more likely to be effective if they are co-ordinated at the international level, as supply chains for communication networks are global and interconnected. No country alone would be able to build the entire supply chain of products and services critical to communication networks from scratch. There is a need for increased co-operation to support demand for trustworthy supply chains, as established in the report prepared by the OECD for the G7 on "Fostering economic resilience in a world of open and integrated markets" (OECD, 2021[1]). More specifically, international co-operation could focus on increasing infrastructure supply chain transparency and diversification, as discussed below, as well as on strengthening standard development, as discussed further below.

To take a strategic approach to the development and implementation of policies to enhance the digital security of communication networks, governments need to integrate them as part of their existing digital or cybersecurity national strategies. These strategies are generally supported at the highest level of government and establish appropriate institutional and multi-stakeholder co-ordination mechanisms.

Incentivising network operators to enhance digital security

To address the cross-cutting challenges facing communication networks described above, governments need to incentivise network operators to further adopt and implement existing and emerging digital security good practices, in particular, digital security risk management frameworks based on risk assessment and risk treatment. In addition, the emerging "zero trust" model could be used to complement risk management frameworks for the most advanced organisations, as further discussed below.

Operators of communication networks are key stakeholders for the management of digital security risk in communication infrastructure. They are generally considered to be operators of critical activities, given that the potential consequences of digital security incidents could extend far beyond the operators themselves and affect multiple sectors and the society. They generally fall within the scope of public policies to protect critical infrastructure and strengthen the digital security of critical activities. These policies set an acceptable level of risk and create the appropriate incentives or requirements for operators to adjust their risk management accordingly. They typically intend to encourage operators to adopt security measures to ensure resilience, which is the ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions (NIST, 2018[161]). These policies also consider potential interdependencies across sectors and borders, such as when a possible incident in one sector can cascade to another or propagate to (or come from) another country.

At the same time, public policies should not create unnecessary burdens for operators, for example by slowing down investments and innovation. The 2019 OECD Recommendation on Digital Security of Critical Activities provides high-level guidance for policy makers to address this challenge, regardless of the critical sector at stake (OECD, 2019[162]). This includes guidance with respect to the overarching policy framework that governments need to put in place in this area, the measures that they should encourage operators of

critical activities to take, the need to establish sustainable trust-based partnerships and the establishment of international co-operation (OECD, 2019[162]).[18]

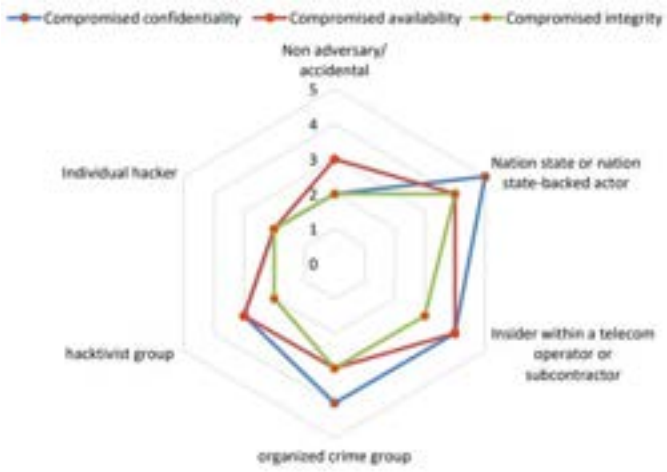
Adopting comprehensive risk management frameworks

Digital security risk management is a holistic and cyclical business process rather than only a technical issue. At a high level, digital security risk management can be divided into two processes: i) risk assessment, i.e. the evaluation of the likelihood and severity of the risk, based on the context, and ii) risk treatment, i.e. business decisions addressing this risk by deciding how much of the risk to accept, mitigate, transfer or avoid (OECD, 2015[163]). Furthermore, to cope with the dynamic nature of threats, vulnerabilities, technologies and other factors, risk management needs to be applied as a cyclical and systematic process. Risk management frameworks allow organisations to take security measures that are appropriate to and commensurate with the risk identified, aligned with their internal risk tolerance (also called "risk appetite") and economic and social interests. According to some experts, and as in other industries, some network operators have not yet fully adopted such an integrated risk management approach in the way they address digital security, and take a more technical, checklists or compliance-based approach.

Network operators should be encouraged to undertake comprehensive risk assessments. The European Union's five-step risk assessment process for 5G networks, outlined below, provides an example of how operators could undertake such risk assessment (NIS Cooperation Group, 2019[38]).

1. Assessing the threat level. Communications networks are increasingly a target of malicious activity. Figure 5 provides an example of a threat assessment done in the EU.

Figure 5. Example of a threat assessment for 5G networks in the European Union



Note: This diagram provides an assessment of the threat level attributed to each threat actor and for each dimension of the impact of the digital security incident (availability, integrity and confidentiality).
Source: NIS Cooperation Group (2019[38]), *EU coordinated risk assessment of the cybersecurity of 5G networks*, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

2. Identifying assets and assessing their criticality. Risk treatment should focus in priority on those assets whose role is considered critical or high. The importance of asset identification will grow significantly as both the sheer number and diversity of devices connected to communication networks are expected to significantly increase. Table 2 provides an example of how stakeholders identified assets in communication networks and assessed their criticality in the European Union.

Table 2. Example of identifying assets and assessing their criticality in 5G networks in the European Union

Type of asset	Core network functions	NFV management and network orchestration (MANO)	Management systems and supporting services (other than MANO)	Radio Access network	Transport and transmission functions	Internetwork exchanges
Criticality	Critical	Critical	Moderate / High	High	Moderate / High	Moderate / High

Source: NIS Cooperation Group (2019[38]), *EU coordinated risk assessment of the cybersecurity of 5G networks*, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

3. Identifying and assessing potential vulnerabilities, including in the supply chain of communication network operators**.** The EU risk assessment considers three main categories of vulnerabilities:

- Vulnerabilities related to the products used in communication networks (e.g. hardware and software) and to processes and policies in place within the operator's organisation. Such vulnerabilities may include a lack of security controls, insufficient monitoring practices, insufficient maintenance of products, a lack of compliance with standards or poorly designed network architectures.
- Supplier-specific vulnerabilities. To assess these vulnerabilities, a risk-profile needs to be attributed to each supplier, including the risk of foreign States' interference and the ability of the supplier to provide its products and services over time, in various scenarios.
- Vulnerabilities stemming from dependency on some suppliers. A lack of diversity in the equipment and solutions used within communication networks and a high degree of reliance on a single supplier (monoculture) creates a dependency on specific solutions and makes it more difficult to procure solutions from other suppliers, especially where solutions are not fully interoperable.

4. Elaborating risk scenarios. Based on the previous steps, stakeholders should elaborate specific risk scenarios for communication networks that connect threats, assets and vulnerabilities together in practical, real-life situations. Such scenarios should include specific risk ownership allocations, in order to clarify responsibility, in particular in the context of the growing complexity of network architecture and of the communication infrastructure supply chain. For example, such scenarios can be based on threat actors exploiting insufficient security measures, supply chain vulnerabilities as well as interdependencies between communication networks such as 5G and other critical sectors.

5. Putting in place mitigating and monitoring measures**.** Based on the previous steps, stakeholders should mitigate key vulnerabilities and decide on the most appropriate risk treatment for each scenario.

Network operators should then use the results of the risk assessment to decide how to best to address the risk (i.e., decide what to do in light of their risk appetite/tolerance). This process is known as risk treatment. They can:

- Reduce it to an acceptable level ("residual risk") by adopting security and resilience measures;
- Take the risk and face the possible consequences;
- Transfer it, for example, by purchasing insurance; or
- Avoid it by not carrying out the activity.

While some network operators may already implement risk assessment and treatment, the rhythm of cyclical risk reviews may need to increase to cope with the aggravating threat landscape. Network

operators' suppliers also need to integrate digital security risk management in the entire lifecycle of their products, from design and development to vulnerability treatment and responsible end-of-life policies (OECD, 2021[91]). The Secure Development Lifecycle (SDL) process is a good example of how suppliers can integrate digital security risk management optimally throughout the life of a product (Microsoft, 2023[164]).

Exploring the potential of zero-trust approaches

In the medium term, governments could consider encouraging network operators to explore the possibility to adopt more advanced security approaches such as the "zero trust" model. While still emerging, the "zero trust" model is based on the almost two decade-old recognition that the perimeter-based digital security approach is no longer effective in modern networks (SC Magazine, 2004[165]; The Open Group, 2021[166]). Perimeter security assumes that networks and assets are best protected by preventing threats from entering the network perimeter. Therefore, trust is implicitly granted to assets or user accounts based on their network location, i.e. trusted within the perimeter, not trusted outside.

The zero trust security model rather operates on a "never trust, always verify" mode, assuming that an attacker is present in the environment and will move laterally to compromise additional assets until the attacker reaches its ultimate objective. Zero trust assumes that an enterprise-owned environment is no more trustworthy than any non-enterprise-owned environment, such as the Internet. It recognises the *de facto* de-perimeterisation resulting from the ever-growing reliance of information systems on external entities (e.g. cloud services, managed service providers), as well as sophistication of threats and multiplication of vulnerabilities.

In a zero trust environment, if a software or hardware product is compromised, the damage can be contained. Enterprises that adopt the zero trust model assume no implicit trust and continually analyse and evaluate the risk to their assets and business functions, and then enact protections to mitigate this risk (NIST, 2020[167]). Zero trust architecture embeds comprehensive security monitoring, granular risk-based access controls and system security automation in a co-ordinated manner throughout all aspects of the infrastructure to focus on protecting data in real-time within a dynamic threat environment (US Government, 2021[168]).Zero trust allows users to access only the bare minimum they need to meet their requirements on a case-by-case basis. It emerged relatively recently because technologies have become mature enough to enable continuous and systematic authentication and monitoring in real-time.

The zero-trust model could therefore strengthen the implementation of digital security risk management in communication infrastructure. In particular, it could help address, at least partly, some of the key challenges identified above, such as the growing complexity of both the network architecture and the supply chain. To be effective, zero trust requires network operators and service providers to have enhanced visibility on the network, i.e. to identify all assets across systems and to monitor traffic and data flows in real time. Virtualisation, software-defined, cloud-based networks as well as the evolution towards more openness (e.g. open architectures such as open RAN and "white box" hardware) could enhance operators' ability to better identify their assets and monitor traffic in real time, thereby facilitating the deployment of zero trust.

Zero trust is a model to implement digital security risk management more efficiently and systematically at the technical level, rather than an alternative to risk management. Therefore, network operators willing to adopt zero trust need to do so on top of state-of-the-art risk management processes. Furthermore, many aspects of zero trust require significant investments and a skilled workforce which many network operators are likely to lack in-house in the short term. Therefore operators need to carefully assess the substantial efforts required to implement zero trust, and consider an incremental approach, focusing on key assets first, one business process as a time, rather than rapidly transitioning the entire system to the model (NIST, 2020[167]).

While zero trust can make risk management more effective, it is exposed to specific threats. For example, a zero trust architecture relies on policy engine and policy administrator components which approve

communication between resources. Their subversion, misconfiguration, or unavailability could compromise the security of these resources (NIST, 2020[167]). More generally, the implementation of zero trust creates another layer of complexity for the purpose of security, which adds to the existing technical complexity inherent to communication networks. Complexity being the enemy of security, this suggests that if not strictly implemented and monitored, zero trust may be counterproductive in certain cases. Currently, zero trust seems to be an option for the most security-mature network operators to consider rather than a realistic immediate option for all.

Overall, the zero trust model is still emerging, and it is therefore too early to draw definitive conclusions on its benefits and challenges. The growing interest in zero trust as a useful security model for operators of critical activities may thus warrant a more in-depth discussion expanding beyond the scope of this paper.

Addressing supply chain digital security risk

The complexity of the communication infrastructure supply chain is increasing, as is the role of certain suppliers in managing digital security risk. To address these challenges, there is a need for governments to incentivise and encourage private stakeholders to i) increase supply chain transparency with respect to digital security evaluation and traceability of components, amongst others, and ii) support its diversification.

The evolution of the communication industry towards more openness exemplifies the support for more supply chain transparency and diversification. For example, open RAN has the potential to increase transparency by further enabling the use of “white box” hardware equipment. It can also increase supply chain diversification by facilitating the entry of new suppliers on the market (e.g., system integrators and open RAN software providers), by providing networks operators a greater choice of products and services and enabling them to easily switch between different suppliers. However, to be fully effective, the potential benefits of more openness in communication networks are likely to require more co-operation across the supply chain, a dynamic industrial ecosystem and digital security to be appropriately valued by stakeholders, in particular compared to other economic objectives such as technical performance or affordability.

Increasing supply chain transparency for digital security

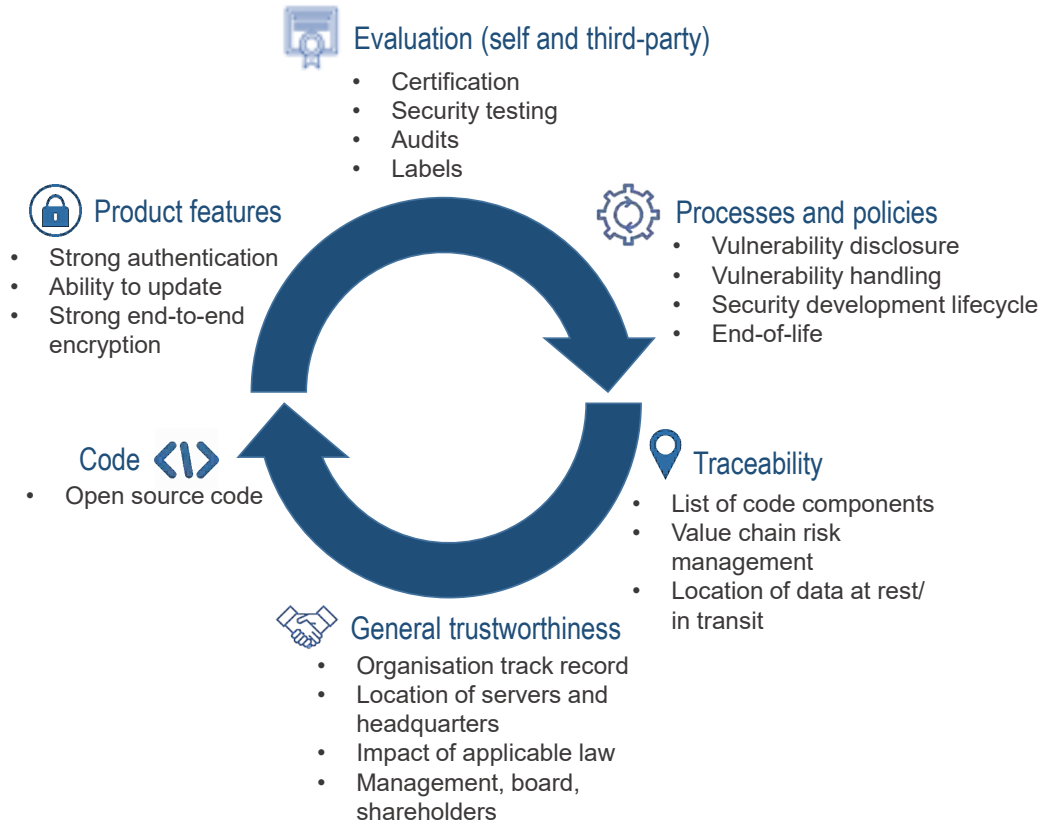
To address supply chain digital security risk, governments can incentivise suppliers to take measures that would increase transparency, in particular to reduce the information asymmetries facing network operators and better equip them to accurately assess digital security risk from their supply chain.

Supply chain transparency refers to cases where relevant information for digital security is made available to all stakeholders in a standardised format, which allows for a common understanding as well as comparability of products and services regarding their level of digital security (OECD, 2021[135]). Significant information asymmetries often prevent network operators from making informed and risk-based decisions regarding their choice of suppliers, e.g. communication equipment vendors, providers of software, as well as cloud and managed services (OECD, 2021[135]). Increasing transparency about digital security of products and services is also a vital tool to make market mechanisms more effective and to improve traceability and accountability. In addition, increasing product transparency is often considered to be a way to mitigate potential vulnerabilities, for instance backdoors that could be inserted in telecom equipment (NL Times, 2021[169]). For instance, empowering digital security experts, both within or outside the government, to access and review source code may reinforce trust in the products and services used in communication networks’ supply chains.

Figure 6 outlines five areas where suppliers can increase transparency: evaluation (self and third-party), product features, process and policies, source code, traceability, and general trustworthiness (OECD, 2021[135]). Governments can also incentivise stakeholders to take action; concrete examples of initiatives

taken to increase supply chain transparency are further discussed below, including in particular the recent interest for developing Software and Hardware Bill of Materials (SBOM and HBOM).

Figure 6. Areas of focus to increase transparency



Note: Examples are provided only for illustrative purposes, and do not aim to be exhaustive or applicable to each product category and context. Suppliers can take action in each of these areas to increase the transparency of the infrastructure supply chain. Governments can also incentivise stakeholders to take action, for instance by mandating certification and traceability for certain products, as discussed below.
Source: OECD elaboration based on OECD (2021[135]), *Enhancing the digital security of products: a policy discussion*, https://doi.org/10.1787/20716826.

Supporting supply chain diversification to reduce market concentration

Supply chain digital security risk can also occur if there is a high market concentration in specific segments of the supply chain of communication networks, which limits the choice of suppliers and, consequently, the choice of digital security solutions for these segments available in the market. Establishing whether market concentration exists in a particular part of the communication network supply chain requires a sound definition of the relevant market. Based on this market definition, the level of concentration can be assessed, ideally relying on different measures of market concentration (e.g. players, activity, revenue etc.).

The most prominent discussion of a potential market concentration in the communication network supply chain is currently taking place in the mobile communication equipment market, in particular with respect to the deployment of 5G networks. Open RAN is put forward as a potential way to address this issue as opening the RAN interfaces allows operators to select different vendors according to their needs (for more details see the discussion on Open RAN and its security implications above). Opening these interfaces may facilitate market entry to new players and thus a diversification of vendors in this market segment.

While the discussion is still at an early stage and while it is too early to evaluate market entry, some stakeholders suggest that diversification can contribute to enhance digital security in several ways. If many suppliers compete and *if digital security is sufficiently valued by network operators*, suppliers are likely to be incentivised to further invest in security. The level of digital security of products and services could then act as a differentiating factor in the market. Supply chain diversification also reduces dependencies on a few suppliers, which can constitute a systemic risk in case the reliance on a single product or supplier (monoculture) becomes or remains prevalent across the communication infrastructure supply chain.

However, supply chain diversification alone is insufficient to ensure appropriate digital security risk management by stakeholders in a specific market. In particular, the positive effects of supply chain diversification may be limited in case of significant information asymmetries and misaligned market incentives (OECD, 2021[135]). As a result, governments willing to address supply chain digital security risk should pursue both objectives in parallel: increasing supply chain transparency and supporting its diversification. Supporting supply chain diversification should therefore be understood as one policy objective amongst others, e.g. empowering network operators to enhance digital security.

Policy actions and country initiatives around the OECD

To achieve the three objectives discussed above, governments can take a wide array of policy actions. This section discusses six categories of policy action: voluntary frameworks, multi-stakeholder initiatives, standards development, third-party evaluation, public procurement, and legal requirements.

These policy actions are introduced below from the least disruptive ("light-touch") to the most interventionist approach for the market. They are versatile and can be tailored to address one or more of the high-level challenges outlined above. For example, governments could develop voluntary frameworks tailored to address the expanding attack surface by focusing on risk assessment/risk treatment methods, end-to-end security and digital risk management throughout the product lifecycle. Similarly, voluntary frameworks could address supply chain risk by establishing a set of best practices for network operators to manage digital security risk from their supply chain.

When deciding which policy actions to apply, policy makers should adopt a balanced approach, between "over-regulation" (i.e. disproportionate policy measures) and "under-regulation" (i.e. the assumption that market dynamics on their own will "naturally" solve public policy challenges). In fact, a mix of policy actions is required to achieve policy objectives and there is no "silver bullet". When devising policy actions, governments should also consider balancing digital security with other important policy objectives such as growth, well-being, cost-effectiveness, privacy and technical efficiency, fostering multi-stakeholder co-operation to consider various viewpoints, and regularly reviewing policy tools, as market conditions and other factors can evolve relatively rapidly (OECD, 2021[135]).

Provision of voluntary frameworks and guidance

Governments can develop and promote voluntary frameworks and guidance on how to better manage digital security risk in communication network infrastructure. These can take the form of sets of principles or more detailed requirements proposed by the government or other institutions, such as standardisation organisations. Such guidance can apply to network operators, as well as to their key suppliers.

In Japan, for instance, the government released a new version of its "Information Security Measures Guidelines for Cloud Service Provision" in September 2021, which are designed to empower stakeholders to better manage digital security risk in a cloud-based environment (MIC, 2021[170]). These guidelines were developed through a multi-stakeholder process involving input from various organisations.

In the United States, the National Institute of Standards and Technology (NIST) has developed the NIST Cybersecurity Framework, which provides organisations with a comprehensive yet simple tool to structure their digital security risk management strategy (NIST, 2023[171]).It is widely used within the national

communication networks' industry (see Box 3). More recently, the Cybersecurity and Infrastructure Security Agency (CISA) published an ICT supply chain risk management toolkit to empower stakeholders, including communication network operators, to better manage the digital security risk associated with their supply chain (CISA, 2021[172]).

Box 3. The NIST Cybersecurity Framework

The NIST Cybersecurity Framework was developed in 2014 by the United States' National Institute of Standards and Technology (NIST) and aims to help organisations assess and treat digital security risk. Its goal is to make a widely accessible framework by facilitating the use of existing international standards, guidelines and practices. The NIST Cybersecurity framework focuses on five core security activities or functions, which could provide a structure for organisations' digital security risk management strategy:

- Identify, i.e. develop a mapping of the organisation's systems, people, assets, data, and capabilities. This includes understanding the business context, the resources that support critical functions, and the related digital security risk, which allows an organisation to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
- Protect, i.e. outline appropriate safeguards to ensure the delivery of the most critical functions.
- Detect, i.e. define appropriate activities to identify the occurrence of a digital security incident in a timely manner.
- Respond, i.e. take action and contain the impact of a potential digital security incident.
- Recover, i.e. develop plans for resilience and to restore the capabilities or services that were impaired due to a digital security incident.

The NIST Cybersecurity Framework provides a list of industry and international standards for each activity that may be used by organisations to assess their maturity. NIST is currently planning a "more significant update" to the Framework (CSF 2.0), taking into account the changing technologies and threats, as well as incorporate lessons learned since its inception. NIST aims to launch CSF 2.0 by 2024.

Source: OECD and NIST (2023[171]), *Cybersecurity Framework*, https://www.nist.gov/cyberframework; NIST (2023[173]), *Updating the NIST Cybersecurity Framework – Journey To CSF 2.0*, https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.

The development of voluntary frameworks should include the multi-stakeholder community, from the design to implementation phase, to be most effective. The involvement of relevant stakeholders will enable policy makers to leverage their knowledge and resources and create the conditions for the broad adoption of the framework at a later stage. While their implementation is usually undertaken on a voluntary basis, stakeholders may incentivise other stakeholders to use these standards; for instance, large corporations can require conformity with voluntary frameworks in their contracts and governments can require conformity in their procurement processes (see below). The best format for the framework will likely depend on the context, ranging from principles-based and outcomes-oriented frameworks to more detailed technical requirements.

Voluntary frameworks can be effective at realigning market incentives and reducing misperceptions of risk. They can also enable stakeholders to assess their maturity regarding digital security risk management good practices. Such frameworks are also more flexible than legal requirements and can therefore adapt more quickly to technological change. As they are voluntary, they have little potential for disproportionate use or market distortion. However, depending on the market, other policy tools may be needed in

conjunction. Voluntary guidance can also be provided by the government as a complement to more general legal requirements, thus enabling stakeholders to better understand how to implement those requirements in practice (see (ENISA, 2021[174]) and below). More generally, voluntary frameworks can be a good starting point for governments, as their design is also an occasion to start a dialogue with relevant stakeholders and raise awareness of best practices.

Supporting multi-stakeholder initiatives and funding research

Governments can also partner with industry and civil society, support existing stakeholder-led initiatives, or encourage the creation of new ones, to enhance digital security. Achieving stakeholder engagement with both network operators and their suppliers is essential for any policy action by governments.

Multi-stakeholder initiatives may focus on promoting more transparency, supporting capacity building and providing specialised resources to the community. Governments may support these initiatives through official acknowledgment of the benefits they bring to society, public funding or allocation of other resources, such as facilities or personnel. Multi-stakeholder initiatives may take various formats and several examples can be seen across the OECD.

For example, in the United Kingdom, the government launched a programme to foster the emergence of new solution providers in the telecom supply chain in the UK in June 2021 called “SONIC Labs”, based in London and Brighton, with GBP 1 million (USD 1.23 million)[19] in public funding (Digital Catapult, 2021[175]). The lab enables suppliers of 5G Open RAN to test their products in a commercially-neutral and collaborative environment. The lab is also intended to encourage innovative suppliers to enter the United Kingdom’s communication supply chain and drive innovation in communication networks. It is run by the communication regulator, Ofcom, and digital technology innovation centre, Digital Catapult, and works with a diverse range of suppliers to explore new open approaches to communication networks, in particular open RAN. In December 2021, the UK government announced an additional investment of GBP 15 million (USD 18.5 million) in this project (DCMS, 2021[120]).[20] In addition, the UK Telecommunications Laboratory (formerly the “National Telecoms Labs”) which was announced as part of UK’s government 5G Supply Chain Diversification Strategy will serve as a research and development facility focusing on security, performance and resilience testing of communication infrastructure, involving operators, vendors, government, academia and other relevant stakeholders (DCMS, 2021[120]).

In Germany, the Federal Ministry of Education and Research provided approximately EUR 5.1 million (USD 5.4 million) [21] to fund the project “OTB-5G+” to research and develop an open testbed for 5G technologies and beyond. The project produced solutions that can be quickly adapted and implemented by companies for their application scenarios. Companies and research institutions could thus trial innovative mobile technologies on the testbed in Berlin. In 2021, the Federal Ministry started its 6G initiative with a funding of up to EUR 700 million (USD 736.8 million).[22] The initiative consists of two main pillars. The first pillar is based on research collaborations on 6G and the communications technologies of the future involving outstanding research institutes and universities (6G-life, 6G-RIC, 6GEM and Open 6G Hub) . The solutions being investigated by these academic collaborations have a strong focus on open approaches for future 6G systems, following “security by design” and “privacy by design” principles from an early stage. The second pillar focuses on 6G industry projects that are expected to explore and develop architectures for promising 6G technologies or entire 6G systems. In addition, these projects should exert a noticeable influence on research transfer and the development of international standards. Under this pillar, the 6G-CAMPUS, 6G-CampuSens and 6G-Terafactory projects research efficient and secure 6G campus networks in industrial environments, based on open RAN.[23]

In the European Union, several network operators published a report calling for European Union members to establish more public-private partnerships dedicated to open RAN, for instance testbeds, trials and incubators (Deutsche Telekom, Orange, Telecom Italia, Telefónica, Vodafone, 2021[136]). The report further suggests that these partnerships may be specifically tasked to identify gaps in the open RAN ecosystem,

and that governments may fund “audits for critical open source technologies” (Deutsche Telekom, Orange, Telecom Italia, Telefónica, Vodafone, 2021[136]).

In Finland, the regulator Traficom organised a “5G security hackathon” in 2019 gathering 70 security researchers from 15 countries (Traficom, 2019[176]), followed by another similar hackathon in 2021 (Traficom, 2021[177]). In Brazil, the Cybersecurity Regulation for the Telecommunications Sector, passed in 2020, created a Cybersecurity and Critical Infrastructure Risk Management Technical Group (Anatel, 2020[178]). The group will be co-ordinated by a “Superintendent”, who has been appointed by Anatel, and will include communication service providers “with significant market power” (Anatel, 2020[178]). Representatives of other providers, agencies and entities may also participate (Anatel, 2020[178]). The group will assess trends and emerging threats that may apply to communication networks and services, monitor and recommend to Anatel best practices to protect the digital security of communication networks emerging regionally and internationally, encourage training to improve digital security skills and propose measures for providers to meet the obligations imposed upon them in the regulation, among other actions.

In the United States, the National Telecommunications and Information Administration (NTIA) established the Communications Supply Chain Risk Information Partnership (C-SCRIP) in 2020, a program that provides a platform to share supply chain security risk information with trusted communication providers and suppliers (NTIA, 2020[179]). Other platforms such as sector-based information sharing and analysis centres (ISACs) and computer emergency response teams (CERTs) provide additional avenues to share information and best practices on digital security among key stakeholders. These types of platforms help to support capacity building to mitigate digital security risk.

Open source security is also high on the agenda of several large organisations, which have partnered through dedicated stakeholder-led structures. For instance, several organisations started the Core Infrastructure Initiative in 2014, after the discovery of the Heartbleed vulnerability.[24] The project was launched by the Linux Foundation and has been replaced by the Open Source Security Foundation (Open SSF) (Core Infrastructure Initiative, 2020[180]). The Open SSF aims to improve open source security by building a broader community with targeted initiatives and best practices (OpenSSF, 2023[181]). These initiatives aim to address the insufficient allocation of human and financial resources for maintaining the digital security of open source products that are widely used and critical to the functioning of the Internet. Namely, they aim to address the “tragedy of the commons” faced by open source products, or the situation where limited ownership rights for a resource results in suboptimal maintenance, even though the resource is widely used (OECD, 2021[135]). Other key initiatives in this area include the Linux Foundation’s initiative to enhance security by design in open source projects (Linux Foundation, 2022[182]; Linux Foundation, 2020[183]).

To increase supply chain transparency, some suppliers have established transparency centres (e.g. Huawei (Techcrunch, 2019[184])), along with software and digital service providers (e.g., Microsoft (2023[185]) and Cisco (2020[186])). Transparency centres allow trusted partners and governments to review the company's product’s code, software updates and threat detection rules in a closed environment (Kaspersky, n.d.[187]). While these transparency centres may be perceived as a step in the right direction, they are insufficient in delivering enough supply chain transparency about a product’s level of digital security. Reviewing source code takes time and resources and is effective only for the version of the code being reviewed, which is analysed against known vulnerabilities or backdoor techniques. Furthermore, access to source code is only one area where increased transparency is needed, as shown in Figure 6.

More promising multi-stakeholder partnerships that intend to increase supply chain transparency include the Bill of Material (BOM) initiative. These include both Software (SBOM) (Box 4) and Hardware Bill of Materials (HBOM), to increase the traceability of software and hardware products (OECD, 2021[135]).

Box 4. Software Bill of Material (SBOM): an emerging best practice to increase supply chain traceability

Similar to a list of ingredients, an SBOM is a formal machine-readable inventory of software components and dependencies in a product. An emerging good practice in the industry, SBOM enhances software transparency and improves visibility into software composition and architecture. An SBOM provides information that enhances stakeholders' understanding of the software supply chain and empowers them to track known vulnerabilities. It can form a foundational data layer on which further security tools, practices, and assurances can be built.

In the United States, the National Telecommunications and Information Administration (NTIA) has launched a multi-stakeholder taskforce to support SBOM and incentivise industry adoption. These efforts have led to the identification of three core elements to support basic SBOM functionality:

- Data Fields: documenting baseline information about each software component that should be tracked.
- Automation Support: allowing for scaling across the software ecosystem through automatic generation and machine-readability.
- Practices and Processes: defining the operations of SBOM requests, generation and use.

These elements can serve for continued collaboration and public-private partnerships to refine and operationalize SBOM work.

The Biden Administration has identified SBOM as a priority to drive software assurance and supply chain risk management and SBOM is included in the National Cybersecurity Strategy released in March 2023. The industry has also started to develop SBOM initiatives to increase the traceability of their products.

Sources: NTIA (2021[188]), *SBOM at a Glance*, https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf; OECD (2021[135]), *Enhancing the digital security of products: a policy discussion*, https://doi.org/10.1787/20716826; White House (2021[10]), *Executive Order on Improving the Nation's Cybersecurity*, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; White House (2023[189]), *National Cybersecurity Strategy* ,https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Supporting the development of standards

Policy makers can also help enhance the digital security of communication networks by supporting the work of Standards Development Organisations (SDOs). The role of SDOs in integrating digital security in standards for communication equipment is becoming essential, as described in Box 5. The development and effectiveness of other policy actions, for instance voluntary guidance, legal requirements or certification, often relies on international standards, which highlights the need for SDOs to appropriately value and integrate digital security. For instance, international SDOs such as ISO and ITU-T and regional SDOs such as ETSI are currently developing security standards for the IoT (OECD, 2021[135]). Similarly, the 3rd Generation Partnership Project (3GPP), which convenes seven telecommunication SDOs to develop technical specifications for mobile networks, has a Working Group devoted to security in 5G networks (3GPP, 2022[190]).[25]

In 2021, the G7 Digital and Technology Ministers recognised "the significant and positive role that digital technical standards have in supporting the global economy and society" and expressed their "support for industry-led, inclusive, multi-stakeholder approaches for the development of technical standards" (G7,

2021[191]). The *Framework for G7 Collaboration on Digital Technical Standards*, attached to the G7 Declaration, sets out areas for further collaboration. In particular, it suggests that governments could facilitate multi-stakeholder dialogue and engagement on standards, contribute to their development and support capacity building, for instance through programs facilitating the participation of civil society and SMEs to the development of standards (G7, 2021[192]).

In addition, governments can also engage with SDOs to ensure that the development process of standards and technical specifications upholds the principles of openness, transparency, multi-stakeholder engagement, inclusiveness and consensus-based discussion. A lack of transparency and diversity in stakeholder participation could lead to structural biases and could allow dominant market players to unduly influence the development process. While acknowledging the industry-led nature of technical development processes, there is a need for governments to engage in a dialogue with SDOs to ensure the effective implementation of these principles, including for relatively new organisations focusing on increasing the openness of communication networks, e.g. through open RAN.

Box 5. The role of Standard Development Organisations (SDOs) in the digital security of communication networks

Over the past decades, SDOs have played an essential role in the development of standards for communication networks and have helped accelerate digital transformation. Technical standards have a significant macroeconomic impact, as they enable products and systems to be more interoperable, unleash innovation (e.g. through standard-essential patents), increase transparency (e.g. through certification mechanisms) and foster competition, including for SMEs.

In the area of communication networks' standards, the following SDOs play a key role:

- Global SDOs, such as the standardisation sector (ITU-T) of the International Telecommunication Union (ITU), the specialized agency of the United Nations for ICTs.
- Regional SDOs, such the European Telecommunications Standards Institute (ETSI).

Ad-hoc partnerships, such as the Internet Engineering Task Force (IETF) and the 3rd Generation Partnership Project (3GPP), bring together national and regional SDOs, including ETSI, TTC (Japan), TTA (Korea), ATIS (USA) and CCSA (People's Republic of China). While technical standards are primarily developed to increase interoperability and technical performance (e.g. reliability and usability), the need to increase confidence and trust in communication networks and to ensure digital security (e.g. through "security-by-design") is increasingly considered as a key objective of standard development processes.

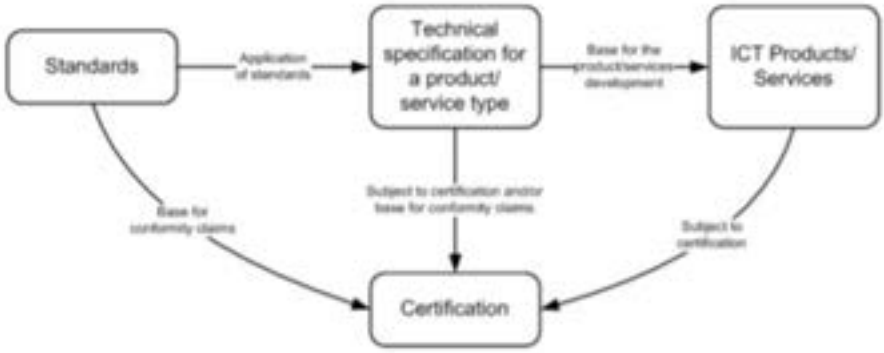
Source: OECD.

Promoting third-party evaluation and certification

In addition to internal self-evaluation by private stakeholders, policy makers can also promote third-party evaluation, such as certification and conformity assessment, to provide more certainty regarding the trustworthiness of products and services used in the supply chain of communication networks. In the United States, a report recommended the creation of a "National Cybersecurity Certification and Labelling Authority, empowered to establish and manage a program on security certifications and labelling of ICT products" (Cyberspace Solarium Commission, 2020[193]). In the European Union, the EU Agency for Cybersecurity (ENISA) is currently in the process of designing a candidate certification scheme on 5G security (ENISA, 2021[194]).

Conformity assessments can be defined as mechanisms to evaluate whether products, processes or organisations meet specific requirements, which can be defined through voluntary guidance and technical standards (see, for example, the EU process in Figure 7). The definition of certification varies across sectors and OECD countries. Experts usually define certification as a mechanism to assess whether products, processes or organisations meet a certain level of digital security, through evaluation by an independent third-party, which may involve security testing. For instance, in the United Kingdom, the communication regulator, Ofcom, hosts a simulated penetration testing initiative called "T-BEST" that evaluates how well communication operators can detect, contain and respond to a cyberattack and identifies key areas of weaknesses (Ofcom, 2023[195]). T-BEST does not grant a score or a "pass" mark, but rather enables operators to identify and address vulnerabilities in their processes, functions or systems.

Figure 7. The EU certification process for ICT products, services and processes



Source: OECD (2021[135]), *Enhancing the digital security of products: a policy discussion*, https://doi.org/10.1787/20716826.

Certification and conformity assessments are widely used in some sectors (e.g. food, energy, industry), including communications, to reduce information asymmetries and ensure that products meet a certain level of quality or safety. They can be effective tools to build trust, increase transparency and promote innovation and competition. Certification of communication equipment or declarations of conformity are widely used in the communications sector to prove a device's adherence to technical specifications and standards to allow the safe operation of communication devices and limit harmful interference to radio services. For example, in the United States, certain radiofrequency devices with the greatest likelihood to cause harmful interference to radio services must follow a more rigorous certification procedure, while other radio frequency devices (depending on their function) can follow a procedure to receive a supplier's declaration of conformity (SDoC) (FCC, n.d.[196]). While certification in the communication sector currently focuses on technical aspects of a device's operation (e.g., to manage interference or adherence to operating conditions), it could be extended to digital security technical requirements. Certification and conformity assessments can incur significant costs for suppliers (OECD, 2021[135]).

Certification schemes are often recognised within a specific jurisdiction. A company would therefore have to undergo new certification processes for every new market they intend to target, which may incur significant additional costs. Cross-border recognition can support the "business case" for certification, as companies would need to go through only one process to obtain a certification that would be valid for a larger market. The EU Cybersecurity Act lays down cross-border mutual recognition of certifications across EU countries. More broadly, there may be a need for countries to further develop cross-border recognition of certification and enhance regulatory interoperability. Importantly, certification and conformity assessments should rely on objective and measurable criteria (OECD, 2021[135]).

Labels can be used to communicate the results of conformity assessments and certification. They can be displayed on the product's package or on the producer's website. Labelling models include information-only (e.g. list of ingredients, for instance a software bill of materials (SBOM)), binary (e.g. "seal of approval"), traffic lights and graded schemes. They can be awarded by public authorities or industry-led organisations. Some labelling schemes include certification as a criterion for awarding the label (OECD, 2021[91]).

To increase the digital security of communication networks, governments may foster the use of certification, for instance by requiring network operators to only buy communication equipment that has been certified following a national or regional certification scheme (see the subsequent section on legal requirements). In Japan, under the "Act on Promotion of Development, Supply and Deployment of Specified Advanced Information and Communication Technology Utilisation Systems" the government provides certain financial benefits (e.g. incentives and tax benefits) to companies developing and supplying 5G equipment that adheres to certification criteria on security, supply and openness (Deutsche Telekom, Orange, Telecom Italia, Telefónica, Vodafone, 2021[136]). The government of Japan also provided a testing environment to test interoperability between several vendors (Deutsche Telekom, Orange, Telecom Italia, Telefónica, Vodafone, 2021[136]).

However, certification does not guarantee that the product withstands any incident. In particular, software-based products require frequent updates and can include millions of lines of code, making it difficult to certify their security over time. For governments, certification should therefore be considered as one policy tool amongst others, which can be used to assist stakeholders in strengthening their digital security risk management approach.

Leveraging public procurement

Another option that policy makers could employ to enhance digital security and foster the adoption of digital security risk management best practices is to require adherence to such best practices in public procurement processes. Suppliers to the government could be required to meet conditions such as adherence to voluntary frameworks and/or a specific best practice, or to digital security requirements specified in procurement contracts. Policy makers would thus support demand for communication equipment products with a higher level of digital security. A recent report in the United States suggested requiring all vendors bidding for public procurement for ICT products to certify their products through recognised standards (OECD, 2021[135]). Additionally, Brazil passed regulation that establishes the minimum cybersecurity requirements for 5G networks that must be observed in all related administrative acts by the federal public administration bodies and entities that are responsible for the implementation of 5G networks (Government of Brazil, 2020[197]). Although this approach creates obligations for some stakeholders, it is less restrictive than the legal requirements discussed below, as it only applies to those businesses supplying to government.

Establishing legal requirements

Legal requirements can be defined as obligations set in laws or regulations, to which stakeholders, such as operators and suppliers, must comply. Generally, they are considered necessary where risks are underestimated or too critical to be left to be handled by stakeholders (e.g. safety or national security), where there is evidence of market failure (e.g. because of externalities or information asymmetries) or where other policy tools have proved insufficient to address significant gaps. Well-designed legal requirements can be a very effective policy tool to enhance the level of digital security of communication networks. They have been successfully implemented in other sectors (e.g. food, energy, automobile) to set minimum requirements for products and organisations.

However, disproportionate legal requirements can considerably disrupt markets. In addition, there is often a gap between the speed of innovation and the time legislative bodies need to adapt to these changes,

e.g. by drafting and adopting new laws, or modifying existing ones. It could also be argued that regulations that are too prescriptive or technical may quickly become obsolete, hinder innovation or limit consumer choice. This argument may be particularly valid in communication markets, where technology innovation, for instance in the development of new IoT applications, is so fast that detailed technical regulations could result in "insecurity-by-compliance" after a few years (OECD, 2021[135]).

To address these pitfalls, legal requirements should be technology-neutral, principles-based and outcome-oriented, and accurately balance digital security considerations with other aspects, such as the economic interests of operators, the level of competition and technical efficiency (OECD, 2021[135]). Designing legal requirements based on international standards is also key to limit inconsistencies across jurisdictions. To empower stakeholders to implement legal requirements, policy makers can also publish guidance, as discussed above.

For instance, in January 2020, the European Commission endorsed the NIS Cooperation Group's 5G Toolbox, which provides guidance to EU Member States to respond appropriately and proportionately to existing and emerging risks associated with communication networks (European Commission, 2020[198]). The EU toolbox is grounded in a risk-based approach and aims to ensure that EU Member States establish legal frameworks that enable relevant authorities to restrict, prohibit, and/or impose specific requirements and conditions for the supply, deployment, and operation of 5G network equipment, in a proportionate manner.

Legal requirements for digital security risk management by operators

Governments can impose security requirements on operators (e.g. rules on secure operation and monitoring, obligations of reporting to relevant authorities, regular audits and controls, conformance with technical standards, etc.). For instance, in the EU, communication network operators ("public electronic communications networks") are subject to security obligations through articles 40 and 41 of the European Electronic Communications Code (EECC) (ENISA, 2020[199]). The Code requires network operators to take sufficient technical and organisational measures for digital security and to notify authorities of significant incidents. It also empowers relevant national authorities to audit, investigate and issue binding instructions to network operators (ENISA, 2020[199]). The NIS2 Directive, which entered into force at the start of 2023, will repeal and replace Articles 40 and 41 of the EECC with effect from October 2024, bringing the security requirements for critical sectors into one EU directive, without changing the essence of these requirements.

In Singapore, the government attached requirements related to network design and resilience to winning bidders of its auction of the 2.1 GHz band spectrum (IMDA, 2021[200]). Namely, all 5G standalone networks must adhere to the cybersecurity requirements set out in IMDA Codes of Practice and design their networks from the beginning to uphold six high-level principles on cybersecurity and network resilience (IMDA, 2021[200]).

In 2020, Brazil passed a Cybersecurity Regulation for the Telecommunications sector, which includes mandatory provisions that apply to communication service providers (Anatel, 2020[178]). These include requiring communication service providers to develop and implement a cybersecurity policy, report security incidents to the communication regulator, Anatel, and share that information with other providers, and report on critical infrastructure. More technical requirements also apply, including for communication service providers to change the standard authentication configuration or equipment and undergo vulnerability assessment cycles that are carried out by a qualified independent company (Anatel, 2020[178]). In conjunction, Brazil passed an Act in 2021 that establishes requirements for communication equipment, including regarding software/firmware updates, default settings and attack mitigation, among others (Brazil, 2021[201]). The Act also sets requirements for suppliers of communication equipment, including on support policies, security updates and co-ordinated vulnerability disclosures, among others.

In the United Kingdom, the Telecommunications (Security) Act 2021 was passed on 17 November 2021 (United Kingdom, 2021[202]). The Act establishes a new telecommunication security framework that places

new duties on public telecommunication providers to identify, mitigate and prepare for security compromises. It also gives the government the power to make communication security regulations (secondary legislation) and guidance in the form of codes of practice. The Act provides Ofcom with responsibility for monitoring and enforcing compliance with the new duties and regulations. In addition, it introduces new national security powers for the government to impose, monitor and enforce controls on public communications providers' use of high-risk vendors' goods, services and facilities (United Kingdom, 2021[202]).

Australia passed an amendment to its Telecommunications Act 1997 that came into effect in 2018, called the Telecommunications Sector Security Reforms (TSSR). TSSR establishes Australia's legislative framework to manage "national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities" (Department of Home Affairs, 2022[203]). TSSR introduces obligations on operators, carriage service providers and intermediaries to "do their best" to protect against digital security threats, as well as puts in place certain obligations to report changes to their networks and systems, among other amendments (Department of Home Affairs, 2022[203]). In 2022, the Parliament endorsed the TSSR, while making six recommendations to improve their implementation and address stakeholder feedback received during a Parliamentary review of the TSSR (Parliament of Australia, 2022[204]).

Subsequently, the Security Legislation Amendment (Critical Infrastructure) Act 2021 and the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 were passed in 2021 and 2022, respectively, amending the Security of Critical Infrastructure Act 2018 (Australia, 2021[205]; Australia, 2022[206]). Key provisions of the 2021 Act include expanding the number of sectors covered, including the communication sector, requiring cyber incident reporting and granting the Government power to assist in severe cyberattacks on critical infrastructure assets (Parliament of Australia, 2021[207]). The 2022 Act introduces new risk management obligations and a new framework with enhanced requirements applying to "systems of national significance" (Department of Home Affairs, 2022[208]). These legislative proceedings serve to demonstrate, on the one hand, a more sector-specific approach to digital security (e.g., TSSR), and, on the other, a more unified approach across industrial sectors, focusing on critical infrastructure (e.g., Security Legislation Amendment (Critical Infrastructure) Act 2021 and (Critical Infrastructure Protection) Act 2022).

For further details on some of the legal requirements outlined in this section, please see the Annex on, "Annex 3. Selection of legal requirements for the digital security of communication networks".

Legal requirements for supply chain security

To address the vulnerabilities associated with communication networks' supply chain more broadly, legal frameworks or regulations can be put in place to allow relevant authorities to restrict the supply or use of certain communication equipment for national security reasons. Such legal requirements may apply either to the supplier or the operator. In France, examples of such legal requirements can be found in the "*code pénal"* (e.g. Art. R226) (France, 2019[209]) and in the "*code des postes et des communications éléctroniques*"(e.g. L34) (France, 2019[210]). In Lithuania, screening mechanisms for national security reasons have recently been introduced, and network operators are required to inform the regulator about the manufacturers and suppliers of equipment used in their networks. In Brazil, included in its Cybersecurity Regulation for the Telecommunications sector is a requirement for communication service providers to use products and equipment from suppliers that i) have an established cybersecurity policy and ii) carry out independent audit processes on a periodic basis (Anatel, 2020[178]).

In the European Union, the new NIS 2 Directive requires individual entities to address cybersecurity risks in supply chains and supplier relationships. At the European level, the Directive strengthens supply chain cybersecurity for key information and communication technologies. Member States, in co-operation with the Commission and ENISA, may carry out Union-level co-ordinated security risk assessments of critical

supply chains, building on the approach taken in the context of the Commission Recommendation on the cybersecurity of 5G networks. Another important initiative is the Cyber Resilience Act (CRA), a legislative proposal issued by the European Commission in September 2022. CRA is expected to address some of the challenges of supply chain security and ensure that products with digital elements (hardware and software) present on the European market are sufficiently secure.

Legal requirements typically restrict the sale or use of products for critical functions of communication networks if they are considered to be "high-risk". While there is no internationally agreed definition of "high-risk", the EU NIS Cooperation group (NIS Cooperation Group, 2019[38]) outlined the following elements as possible criteria to attribute a "high-risk" classification. These criteria are mostly based on the likelihood of a supplier being subject to interference from a foreign country:

- A strong link between the supplier and a government of a given third country.
- The third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country. In this context, a higher risk profile may be attributed to suppliers that are under the jurisdiction of third countries conducting an offensive cyber policy.
- The characteristics of the supplier's corporate ownership.
- The ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.
- The supplier's ability to assure supply.
- The overall quality of products and the cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.

Concluding remarks

Communication networks are a key foundation of digital transformation of the economy and society. Ensuring their digital security and resilience has become a priority for policy makers across the OECD. However, both attacks on communication networks and the communication networks themselves are evolving, making it necessary to consider the different ways networks may be changing and their impact on digital security. This report considers four trends that are shaping and changing communication networks and their impact on digital security: i) the increasing criticality of communication networks, ii) the virtualisation of networks and the integration of cloud services; the trend towards more openness in networks; and the use of AI in communication networks. While these trends may enable many benefits to digital security, three cross-cutting challenges emerge, namely an expanding attack surface, a broader and more complex supply chain, and an aggravating and fast-evolving threat landscape, characterised by increasingly sophisticated actors and a commoditisation of attacks.

Within this context, policy makers have a clear role to play to incentivise the adoption of best practices and to support an enabling environment to encourage stakeholders to reach an optimal level of digital security. Governments can consider three key policy objectives: i) adopting a holistic and strategic approach, ii) incentivising network operators to enhance digital security, and iii) addressing supply chain digital security risk by encouraging suppliers to improve transparency and by supporting supply chain diversification. Several policy actions can be applied that uphold these objectives, ranging from light-touch to more interventionist approaches: voluntary frameworks and guidance, multistakeholder initiatives and funding research, third-party evaluation and certification, public procurement, and legal requirements.

Annex 1. Open Source Software in communication networks

Open source software relates to the development of software released under a license that allows anyone to use, study, change and distribute the software and its source code to anyone and for any purpose (Open Source Initiative, 2007[211]). Open source code licenses may impose obligations on users of open source software; for example, a common requirement is to disclose the open source components used in the software being distributed.

The functioning of open source organisations may vary as each project can define its own model, including how the group operates and makes decisions. Common elements usually include defining the code of conduct for engagement and collaboration, the decision-making process, the openness to external contributions and legal considerations, such as trademarks. There are a range of possible models, ranging from centralised control by an individual or an organisation, to distributed control, for example based on contributions (OSS Watch, 2013[212]).

Open source components are common in the software products. For example, according to 2023 industry reports, 96% of codebases contain open source components and 76% of code in codebases is open source (Synopsys, 2023[213]). Communication networks are no exception to the widespread use of open source software: in 2020, 70% of mobile operators globally reported running the Open Network Automation Platform (ONAP) (The Linux Foundation, 2020[214]). ONAP is an open source platform that network operators, cloud providers, and businesses can use to orchestrate, automate, and manage their network and edge computing services, especially for 5G and next-generation networks (Open Network Automation Platform (ONAP), 2023[215]). In December 2022, ONAP released its 11th release, with further enhancements in several use cases, including network slicing, integration with open RAN specifications, and handling cloud-native network functions (ONAP, 2022[216]). As today's communication networks evolve to become more virtualised and reliant on software, as noted in the trends above, the role of open source software in communication networks is likely to grow.

Large equipment manufacturers like Nokia, Ericsson, and Cisco typically integrate open source components into their products, independently of open RAN solutions. Cisco, for instance, reports a sizable list of the various open source components that it has integrated into its products; the company also has founded several open source projects and participated in countless others (Cisco, 2021[217]).

Annex 2. Open RAN initiatives in OECD countries

Open RAN policy initiatives in OECD countries and partner economies

Several OECD countries are supporting the development of open RAN domestically. The United Kingdom established four key "Open RAN Principles" that aim to maximise and achieve the potential benefits of open RAN environments, which are "open disaggregation", "standards-based compliance", "demonstrated interoperability" and "implementation neutrality" (DCMS, 2022[116]). Furthermore, the United Kingdom established the Future RAN Competition (FRANC) to support the development of open RAN products and suppliers and announced 15 winning projects under the FRANC. In total, the winning projects were granted GBP 36 million (USD 44.4 million) in funding (DCMS, 2021[120]).[26] In the United States, the Federal Communications Commission (FCC) issued a Notice of Inquiry on open RAN in March 2021 (FCC, 2021[218]). In addition, the United States established the Public Wireless Supply Chain Innovation Fund, which aims to promote and deploy technology to support "wireless technology supply chains that use open and interoperable interface radio access networks", accelerate commercial deployments of open and interoperable equipment and support the security of equipment in multi-vendor networks, among other goals (Telecommunications Authorization Act, 2022[219]). In Japan, the government introduced a tax incentive in 2020 to promote 5G investment, with requirements of openness, along with security, reliability and stability of provision (MIC, 2020[220]). This measure is extended in fiscal year 2022, with certain updates on the requirements until the end of fiscal year 2024. Germany has also earmarked over EUR 300 million (USD 315.7 million) of its proposed EUR 130 billion (USD 136.8 billion) economic stimulus funding for the development of open RAN technologies (Tech Times, 2021[221]).[27] In Brazil, the National Telecommunications Agency (Anatel) has created an open RAN Technical Group (open RAN TG) to monitor and evaluate the evolution of open RAN technology to inform its regulatory agenda (Anatel, 2022[222]). In support of this aim, Anatel and the University of Brasília (UnB) signed an agreement whereby the University will carry out studies on the implementation of the open RAN architecture in Brazil.

OECD countries have also engaged in partnerships, which include the promotion of open RAN technologies. Australia, India, Japan and the US, or "the Quad", committed to collaborating on several issues, including to advance the deployment of open and transparent mobile networks through approaches such as open RAN (White House, 2021[223]). Under this, the Quad governments launched an industry dialogue for open RAN deployment and adoption and agreed to facilitate its deployment, including by supporting the testing of the technology (White House, 2021[224]). The US and Japan further noted their joint intent to advance open RAN technology, among other topics, under the Competitiveness and Resilience Partnership (White House, 2021[225]). In addition, Korea and the US committed to working together on several emerging technologies, including open RAN, in a joint Leaders' Statement (White House, 2021[226]).

Open RAN industry initiatives and developments in OECD countries

There are several examples of industry initiatives related to open RAN, including planned deployments. Building on Rakuten Mobile's experience, 1&1 AG and Rakuten signed a partnership to jointly build Germany's fourth mobile network, which will be fully virtual and based on open RAN technology (Rakuten, 2021[127]). Following suit, in June 2021, DISH Network announced its partnership with Dell Technologies to support its plans to launch a "greenfield" 5G network based on open RAN technologies, aiming to be the first network to deploy open RAN technology in the United States (DISH Network Corporation, 2021[128]). Dell will provide edge compute and RAN infrastructure to support DISH's deployment. In June 2021, Vodafone selected six vendors with whom it will build Europe's first open RAN network and further announced in January 2022 that its first 5G open RAN site has been turned on in the UK, the first of a total of 2 500 planned sites in the country (Vodafone, 2021[227]), (Vodafone, 2022[228]). Further examples of industry action regarding open RAN, including memorandums of understanding, co-operation agreements, trials, testing, R&D centres, and deployments can be found in Annex Table 2.1.

Annex Table 2.1. Selected examples of industry open RAN initiatives around the OECD

Type of Initiative	Industry Stakeholder(s) involved[1]	Date	Details
R&D Centre/ Testing facility	NEC Corporation	November 2020	NEC Global open RAN Centre of Excellence (UK)
	Mavenir	April 2021	Development Centre for open RAN Radio software (UK)
	Mavenir	November 2020	Open RAN Centre of Innovation (UK)
	Nokia	June 2021	O-RAN Collaboration and Testing Centre (US)
	IBM	February 2021	Open RAN Centre of Excellence (Spain)
	Ericsson	March 2021	Ericsson Open Lab to collaborate with Ericsson customers and partners on network virtualisation, incl. open RAN technologies (Canada and virtual)
	Telecom Italia (TIM)	June 2021	Open Test and Integration Centre Lab, based within its Innovation Lab in Turin (Italy)
	OpenLab i14y	November 2021	Open RAN lab for testing and integrating disaggregated network components to accelerate the time-to-market of Open RAN solutions. 17 million EUR through public funding by the German government; 17 million of additional funding through a consortium of companies and research institutes (Germany)
	Orange	November 2021	Open RAN Integration Centre
	Vodafone	April 2021	Open RAN Test and Validation Lab (UK)
	Vodafone	May 2021	Global competence centre for R&D and innovation, including on open RAN solutions (Germany)
	Vodafone	January 2022	R&D centre for open RAN microchip design (Spain)
	Parallel Wireless	September 2021	Open RAN R&D Centres (US, UK, Israel)
	KT Corporation and Fujitsu	January 2022	Verification facility at KT R&D Centre in Seoul (South Korea)
	Rakuten Symphony (subsidiary of Rakuten Mobile)	February 2022	Announced expansion of operations in France, Germany and UK (including R&D and engineering labs and a new French branch) to promote the adoption of open RAN in Europe
Memorandum of Understanding (MoU)	TIM, Deutsche Telekom, Orange, Telefónica and Vodafone	February 2021 (TIM) January 2021 (others)	MoU to promote, develop and implement open RAN technologies in Europe

	Telefónica and Rakuten Mobile	September 2020	MoU to cooperate to advance open RAN technologies, 5G and operations support systems
	Rakuten Mobile and Fujitsu	May 2021	MoU to collaborate to develop open RAN solutions for global market
	Rakuten Mobile and NEC	May 2021	MoU to collaborate to develop open RAN solutions for global market
	KT Corporation, NTT DOCOMO and Fujitsu	January 2022	MoU to cooperate to develop open RAN ecosystem, including to build additional testing facilities for O-RAN and interoperability testing
Co-operation agreement	NTT DOCOMO, Dell Technologies Japan Inc., Fujitsu Limited, Intel K.K., Mavenir, NEC Corporation, NTT DATA Corporation, NVIDIA, Qualcomm Technologies, Inc., Red Hat, VMware K.K., Wind River and Xilinx, Inc.	February 2021	13 companies agreed to cooperate towards the development of the "5G open RAN Ecosystem" and the acceleration of implementation
Deployment/planned deployment	NTT DOCOMO	Since its 4G deployment	Deployment of 4G to 5G networks with open interface
	Rakuten Mobile	2020	Deployment of greenfield 4G network with open virtualised distributed RAN began in March 2020; by February 2022 Rakuten's network reached 96% coverage of Japan's population
	Deutsche Telekom	2021	Switched on "O-RAN Town" in Neubrandenburg, Germany, a live open RAN deployment
	1&1 and Rakuten Mobile	2021	Partnership to jointly build a virtualised open RAN mobile network (Germany)
	DISH Network	2021	Partnering with Dell Technologies to deploy a cloud-native 5G network based on open RAN technologies
	Vodafone	2021 2022	Selected partners to deploy its open RAN network (2021) and later announced the switch-on of the first of 2 500 planned 5G open RAN sites in the UK (2022)
	TIM	2021	TIM's open RAN network launched in Faenza, Matera and Saluzzo
	Verizon	2021	Announced that by end 2021, its suppliers would provide open RAN compliant equipment to support its 5G deployments in C-band and mmWave
	Millicom (Tigo)	2021	Partnering with Parallel Wireless to deliver 4G open RAN, beginning with 362 sites in rural Colombia
	Fraunhofer IIS (research institute)	2020	Announced deployment of 5G private network based on O-RAN Alliance specs at its Erlangen and Nuremburg sites
	Telefónica	2021	Partnering with NEC to conduct pre-commercial trials in Brazil, Germany, Spain and UK, aiming to reach 800 sites ready for commercial use by early 2022 Activated open RAN mini-radio cells in 2022 in Munich
	AT&T	2021	Conducted trial and demos on open fronthaul using O-RAN specs and expects to include O-RAN compliant equipment in network during 2022

Note: Please note that the above list is meant to provide additional examples of recent open RAN initiatives around OECD countries and is not intended to be exhaustive. "R&D" refers to research and development efforts. For industry deployments, only the primary mobile network operator is listed, not all of the suppliers that may have contributed to the open RAN deployment. The only except to this is if the network deployment constitutes a partnership.
Source: OECD elaboration based on information from industry stakeholders' websites.

Annex 3. Selection of legal requirements for the digital security of communication networks

The European Electronic Communications Code (EECC)

In the EU, communication network operators ("*public electronic communications networks*") are subject to security obligations through articles 40 and 41 of the European Electronic Communications Code (EECC), adopted in 2018 (ENISA, 2020[199]). The directive states that Member States shall ensure that:

- Communication network operators:
  - "Take appropriate and proportionate technical and organisational measures" to "manage the risks posed to the security of networks and services", taking into account "the state of the art", including "encryption where appropriate", in order to "prevent and minimise the impact of security incidents on users and on other networks and services".
  - "Notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services".
  - "Inform their users potentially affected" by a digital security incident as well as "of any possible protective measures or remedies which can be taken by the users".
- Competent national authorities:
  - Have the power "to issue binding instructions" to communication network operators.
  - Have the power to require communication network operators to "provide information needed to assess the security of their networks and services, including documented security policies" to "submit to a security audit carried out by a qualified independent body or a competent authority and make the results thereof available to the competent authority".
  - Have the power "to investigate cases of non-compliance and the effects thereof on the security of the networks and services".
  - Have the power "to obtain the assistance of a Computer Security Incident Response Team ('CSIRT')".
  - Where appropriate, "consult and cooperate with the relevant national law enforcement authorities".

ENISA, the EU Agency for Cybersecurity, published guidance in order to assist EU Member States and stakeholders in the implementation of articles 40 and 41 of the EECC and to facilitate harmonisation across EU countries (ENISA, 2021[174]). This highlights the benefits of combining several policy tools to enhance the digital security of communication networks (in this case, legal requirements and voluntary guidelines). This voluntary guidance details practical steps that communication networks operators can take to comply the law, on the basis of 8 domains (D) and 29 security objectives (SO):

- D1: Governance and Risk Management.
  - SO1: Information security policy.
  - SO2: Governance and risk management.
  - SO3: Security roles and responsibilities.
  - SO4: Security of third party dependencies.
- D2: Human Resources Security.

    - SO5: Background checks.
    - SO6: Security knowledge and training.
    - SO7: Personnel changes.
    - SO8: Handling violations.
- D3: Security of Systems and Facilities.
    - SO9: Physical and environmental security.
    - SO10: Security of supplies.
    - SO11: Access control to network and information systems.
    - SO12: Integrity of network and information systems.
    - SO13: Use of encryption.
    - SO14: Protection of security critical data.
- D4: Operations Management.
    - SO15: Operational procedures.
    - SO16: Change management.
    - SO17: Asset management.
- D5: Incident Management.
    - SO18: Incident management procedures.
    - SO19: Incident detection capability.
    - SO20: Incident reporting and communication.
- D6: Business Continuity Management.
    - SO21: Service continuity strategy and contingency plans.
    - SO22: Disaster recovery capabilities.
- D7: Monitoring, Auditing and Testing.
    - SO23: Monitoring and logging policies.
    - SO24: Exercise contingency plans.
    - SO25: Network and information systems testing.
    - SO26: Security assessments.
    - SO27: Compliance monitoring.
- D8: Threat Awareness.
    - SO28: Threat intelligence.
    - SO29: Informing users about threats.

For each SO, the ENISA guidance provides examples of technical and organisational measures that communication networks can take, as well examples of evidence that can be provided to the competent national authority by the communication network operator, in case of an audit.

Singapore's legal requirements attached to spectrum auctions

In Singapore, the regulatory authority, the Infocomm Media Development Authority (IMDA) attached requirements related to network design and resilience to winning bidders of its recent auction of 2.1 GHz band spectrum (IMDA, 2021[200]). Namely, all 5G standalone networks must adhere to the cybersecurity requirements set out in IMDA Codes of Practice. The IMDA's Telecommunications Cybersecurity Code of Practice requires ISPs to adhere to requirements related to security incident management requirements and detection, response and mitigation of digital security threats (IMDA, 2021[229]). The code bases its

requirements on international standards and best practices, including from the International Organization for Standardization (ISO) and the IETF. In addition to adherence to the Codes, winning bidders of the auction must design their networks to adhere to the following six key principles:

- "Defence-in-depth: Adopt security-by-design principles by implementing various defence mechanisms which are secure and scalable (e.g., capability to turn on encryption upon request);
- Zero-trust Environment: Ensure that the 5G network is always secure and trusted through the deployment of network security solutions (e.g., implementing a "demilitarised zone" and other relevant measures);
- Network Element Assurance: Ensure that a risk assessment strategy and policy will be applied to the 5G infrastructure (e.g., through policy compliance with the Network Equipment Security Assurance Scheme currently being defined by 3rd Generation Partnership Project (3GPP) and Global System for Mobile Communications, and demonstrate how security assurance is achieved such as through the security testing of equipment);
- Resilience by Outcome: Demonstrate end-to-end network resilience to minimise outages and impact;
- Minimise Dependency: Configure networks, to the extent feasible, to minimise instances where a failure of the (a) fibre network used to provide broadband services, and/or (b) infrastructure used to provide other mobile services in a geographical area, could also affect 5G services in the same geographical area; and
- Adopt Technology: Use of advanced technologies for resilience purposes, e.g., the use of automation and machine learning to detect, respond and recover from service disruption expeditiously" (IMDA, 2021[200]).

These requirements are included along with other rollout and deployment obligations, along with a commitment to deploy a standalone 5G network using the newly assigned band, and to provide wholesale services under certain conditions (IMDA, 2021[200]). However, the design of spectrum assignment procedures is a delicate process and should be approached with care, as the set-up of the process, including any requirements or commitments to fulfil policy objectives can have an impact on the end result of the auction. For example, in the above auction design, some may argue that IMDA's requirements with regard to network design and resilience could favour incumbents, which may have more expertise and capital to adhere to them. IMDA's requirement to provide wholesale services may have been included to temper this potential foreseen outcome.

Monitoring the adherence to the above digital security obligations may also pose a challenge, as there may be a range of possible actions that could qualify as compliant, depending on the regulator's criteria. Defining and sharing with licensees the specific metrics the regulator plans to use to determine compliance would be helpful for operators.

References

3GPP (2022), *SA3- Security*, https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security. [190]

Accenture and Intel (2021), *Creating far edge networks for emerging ultra-low latency services*, https://builders.intel.com/docs/networkbuilders/creating-far-edge-networks-for-emerging-ultra-low-latency-services.pdf. [233]

Amazon (2021), *DISH and AWS Form Strategic Collaboration to Reinvent 5G Connectivity and Innovation*, https://press.aboutamazon.com/news-releases/news-release-details/dish-and-aws-form-strategic-collaboration-reinvent-5g/. [81]

AMSJ (2021), *Nornickel and Nokia successful testing 5G network at underground mine*, https://www.amsj.com.au/nornickel-and-nokia-successful-testing-5g-network-at-underground-mine/. [11]

Anatel (2022), *OpenRAN*, https://www.gov.br/anatel/pt-br/regulado/certificacao/openran/ (accessed on 15 February 2022). [222]

Anatel (2020), *Resolução nº 740, de 21 de dezembro de 2020 [Resolution no. 740 of 21 December 2020]*, Gov.br, https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740 (accessed on 10 March 2022). [178]

Armis (2020), *URGENT/11. 11 zero day vulnerabilities impacting billions of mission-critical devices*, https://www.armis.com/research/urgent11/. [39]

AT&T (2021), *General Motors and AT&T Set Automotive Connectivity Benchmark with 5G*, https://about.att.com/story/2021/att_gm_5g.html. [80]

AT&T (2019), *AT&T and IBM announce multi-year alliance*, https://about.att.com/story/2019/att_ibm_alliance.html. [65]

AT&T Services, Inc. (2021), *Comments of AT&T in the matter of promoting the deployment of 5G open radio access networks (GN Docket No. 21-63)*, FCC, https://www.fcc.gov/ecfs/document/1042871504579/1 (accessed on 15 February 2022). [130]

Australia (2022), *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*, Federal Register of Legislation, https://www.legislation.gov.au/Details/C2022A00033. [206]

Australia (2021), *Security Legislation Amendment (Critical Infrastructure) Act 2021*, Federal Register of Legislation, https://www.legislation.gov.au/Details/C2021A00124. [205]

AWS (2023), *Telecommunications on AWS*, https://aws.amazon.com/telecom/?nc1=h_ls. [62]

AWS (2021), *We're pushing closer to the edge with AWS*, https://exchange.telstra.com.au/were-pushing-closer-to-the-edge-with-aws/. [76]

AWS (2019), *Announcing AWS Wavelength for delivering ultra-low latency applications for 5G*, https://aws.amazon.com/about-aws/whats-new/2019/12/announcing-aws-wavelength-delivering-ultra-low-latency-applications-5g/. [63]

BBC (2021), *JBS: Cyber-attack hits world's largest meat supplier*, https://www.bbc.com/news/world-us-canada-57318965. [5]

BBC (2017), *South Korean firm's 'record' ransom payment*, https://www.bbc.com/news/technology-40340820. [34]

Bell Canada (2021), *Bell partners with Google Cloud to deliver next-generation network experiences for Canadians*, https://bce.ca/news-and-media/releases/show/bell-partners-with-google-cloud-to-deliver-next-generation-network-experiences-for-canadians. [68]

Bernat, L. (2021), "Enhancing the digital security of critical activities", *Going Digital Toolkit Note, No. 17*, https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf. [160]

Bloomberg (2019), *Vodafone Found Hidden Backdoors in Huawei Equipment*, https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment. [13]

Brazil (2021), *ATO Nº 77, DE 5 DE JANEIRO DE 2021 [Act No. 77]*, DIÁRIO OFICIAL DA UNIÃO, https://www.in.gov.br/web/dou/-/ato-n-77-de-5-de-janeiro-de-2021-297933302 (accessed on 10 March 2022). [201]

Broadband Forum (2019), *Broadband Forum and ONF ease the path to automated and open virtualised access networks*, https://www.broadband-forum.org/2019-10-14-broadband-forum-and-onf-ease-the-path-to-automated-and-open-virtualized-access-networks (accessed on 11 February 2022). [100]

BSI (2022), *Open-RAN Risk Analysis [Open-RAN Risikoanalyse]*, Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/5G/5GRAN-Risikoanalyse.pdf;jsessionid=5A4D3B1E0E523AC3AF51DEF742794950.internet471?__blob=publicationFile&v=5. [138]

BT (2023), *BT uses AWS Wavelength to bring the power of 5G and the cloud to businesses on the move*, BT, https://newsroom.bt.com/bt-uses-aws-wavelength-to-bring-the-power-of-5g-and-the-cloud-to-businesses-on-the-move/. [69]

CISA (2021), *Emergency Directive 21-02*, https://cyber.dhs.gov/ed/21-02/. [158]

CISA (2021), *ICT supply chain risk management toolkit*, https://www.cisa.gov/ict-supply-chain-toolkit. [172]

CISA (2021), *Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm*, https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf. [28]

CISA (2020), *Edge vs. Core - An increasingly less pronounced distinction in 5G networks*, [90]

https://www.cisa.gov/sites/default/files/publications/5g_edge-core-computing_508_1.pdf.

Cisco (2021), *Open source in Cisco products*, https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html (accessed on 30 September 2021). [217]

Cisco (2020), *Transparency Centers*, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-transparency-service-center-faq.pdf. [186]

Cloudflare (2023), *What is the control plane? Control plane vs. data plane*, https://www.cloudflare.com/learning/network-layer/what-is-the-control-plane/. [46]

Core Infrastructure Initiative (2020), *Core Infrastructure Initiative*, The Linux Foundation, https://www.coreinfrastructure.org/. [180]

CSO (2019), *Telcos around the world hit by long-term intelligence gathering cyberattack*, https://www.csoonline.com/article/3405163/telcos-around-the-world-hit-by-large-scale-long-term-intelligence-gathering-cyberattack.html. [37]

Cybereason Nocturnus (2021), *DeadRinger: Exposing Chinese Threat Actors Targeting Major Telcos*, Cybereason, https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos#executive-summary. [9]

Cyberspace Solarium Commission (2020), *Cyberspace Solarium Commission Report*, https://www.solarium.gov/. [193]

Dark Reading (2019), *The Commoditization of Multistage Malware Attacks*, https://www.darkreading.com/vulnerabilities-threats/the-commoditization-of-multistage-malware-attacks. [16]

DCMS (2022), *Open RAN Principles*, https://www.gov.uk/government/publications/uk-open-ran-principles/open-ran-principles. [116]

DCMS (2021), *New measures to boost UK telecoms security*, https://www.gov.uk/government/news/new-measures-to-boost-uk-telecoms-security (accessed on 14 February 2022). [120]

Dell Technologies (2021), *Build a network that's open to change*, https://www.delltechnologies.com/asset/da-dk/products/networking/briefs-summaries/open-networking-point-of-view.pdf (accessed on 29 September 2021). [103]

Dell Technologies (2021), *The Edge – Old, New, Borrowed and Blue*, https://www.delltechnologies.com/en-us/blog/the-edge-old-new-borrowed-and-blue/. [234]

Department of Home Affairs (2022), *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*, Australian Government, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022. [208]

Department of Home Affairs (2022), *Telecommunications sector security*, Australian Government, https://www.homeaffairs.gov.au/nat-security/Pages/telecommunications-sector-security.aspx (accessed on 5 October 2021). [203]

Deutsche Telekom (2021), *Telekom switches on O-RAN Town in Neubrandenburg*, https://www.telekom.com/en/media/media-information/archive/telekom-switches-on-o-ran- [126]

town-in-neubrandenburg-630566 (accessed on 4 October 2021).

Deutsche Telekom AG (2023), *O-RAN Town: Piloting a high-power multivendor open RAN solution in a brownfield network*, Deutsche Telekom AG, https://www.telekom.com/resource/blob/1026848/c75d63ea6a638d02cf56bcb3ebe33c0c/dl-230220-o-ran-en-data.pdf. [230]

Deutsche Telekom, Orange, Telecom Italia, Telefónica, Vodafone (2021), *Building an open RAN ecosystem for Europe*, https://www.vodafone.com/sites/default/files/2021-11/building-open-ran-ecosystem-europe.pdf. [136]

Dialogic innovation & interaction (2020), *Managing AI use in telecom infrastructures: Advice to the supervisory body on establishing risk-based AI supervision*, https://www.dialogic.nl/wp-content/uploads/2020/06/Dialogic-ManagingAIuseintelecominfrastructures.pdf. [142]

Digital Catapult (2021), *Digital Catapult launches new high-tech 5G lab to boost network security and resilience*, https://www.digicatapult.org.uk/about/press-releases/post/digital-catapult-launches-new-high-tech-5g-lab-to-boost-network-security-and-resilience/. [175]

DISH Network Corporation (2021), *DISH and Dell Technologies Will Build the Nation's First Open RAN 5G Edge Infrastructure*, https://about.dish.com/news-releases?item=123509 (accessed on 14 February 2022). [128]

EconomyNext (2020), *Sri Lanka Telecom says dealing with REvil hack, customer data safe*, https://economynext.com/sri-lanka-telecom-says-dealing-with-revil-hack-customer-data-safe-70322/. [35]

Elisa Automate (2020), *A Decade of Experience in Automation*, https://elisaautomate.com/elisa-story/ (accessed on 9 December 2020). [143]

ENISA (2021), *Guideline on security measures under the EECC*, https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc. [174]

ENISA (2021), *Securing EU vision on 5G: cybersecurity certification*, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification. [194]

ENISA (2020), *5G threat landscape*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks. [88]

ENISA (2020), *Security Supervision under the EECC*, https://www.enisa.europa.eu/publications/supporting-the-implementation-of-the-european-electronic-commmunications-code-eecc/. [199]

ENISA (2019), *ENISA Threat Landscape for 5G Networks. Threat assessment for the fifth generation of mobile telecommunications networks (5G)*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks. [36]

ENISA (2012), *Cloud computing: benefits, risks and recommendations for information security*, ENISA, https://www.enisa.europa.eu/media/news-items/cloud-computing-speech. [89]

Ericsson (2023), *Security considerations of Open RAN*, Ericsson, https://www.ericsson.com/en/security/security-considerations-of-open-ran. [107]

Ericsson (2023), *Telecom Security*, Ericsson, https://www.ericsson.com/en/security. [159]

Ericsson (2019), *Automating MIMO - MIMO Machine Learning - Ericsson*, https://www.ericsson.com/en/cases/2019/augmenting-mimo-energy-management-with-machine-learning-and-ai (accessed on 3 August 2021). [151]

Ericsson (2018), *Building 4G sliced networks*, https://www.ericsson.com/en/blog/2018/4/building-4g-sliced-networks. [51]

ETSI (2022), *ETSI releases first O-RAN specification*, https://www.etsi.org/newsroom/press-releases/2120-2022-09-etsi-releases-first-o-ran-specification (accessed on 25 September 2022). [140]

ETSI (2021), *MEC security: Status of standards support and future evolutions*, https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_WP_46-_MEC_security.pdf. [86]

ETSI (2021), *Multi-access Edge Computing (MEC)*, ETSI, https://www.etsi.org/technologies/multi-access-edge-computing. [85]

ETSI (2020), *ETSI GR NFV 003 V1.5.1. Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV*, https://www.etsi.org/deliver/etsi_gr/NFV/001_099/003/01.05.01_60/gr_NFV003v010501p.pdf. [231]

ETSI (2018), *5G Release-15: NG-RAN Architecture description (3GPP TS 38.401 version 15.2.0 Release 15)*, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3219 (accessed on 19 February 2021). [108]

ETSI (2018), *MEC in 5G networks*, ETSI, https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf. [87]

ETSI (2014), *ETSI GS NFV 002 V1.2.1, Network Functions Virtualisation (NFV); Architectural Framework*, https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf. [47]

Eurohealth (2020), *Keeping what works: Remote consultations during the COVID-19 pandemic*, Eurohealth, https://apps.who.int/iris/rest/bitstreams/1313795/retrieve. [25]

European Commission (2021), *A secure and reusable Artificial Intelligence platform for Edge computing in beyond 5G Networks*, https://cordis.europa.eu/project/id/101015922 (accessed on 28 September 2021). [152]

European Commission (2020), *EU Toolbox on 5G security*, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures. [198]

European Commission, Directorate-General for Communications Networks, Content and Technology, Dinges, M., Hofer, M., Leitner, K., et. al. (2021), *5G Supply market trends*, Publications Office, https://data.europa.eu/doi/10.2759/017326. [21]

European Court of Auditors (2018), *Broadband in the EU Member States: despite progress, not all the Europe 2020 targets will be met*, European Court of Auditors, https://op.europa.eu/webpub/eca/special-reports/broadband-12-2018/en/. [19]

eWeek (2020), *NVIDIA Acquires Cumulus to Accelerate Open Networking*, [106]

https://www.eweek.com/networking/nvidia-acquires-cumulus-to-accelerate-open-networking/.

FCC (2021), *FCC seeks comment on Open radio access networks*, https://www.fcc.gov/document/fcc-seeks-comment-open-radio-access-networks-0 (accessed on 4 October 2021). [218]

FCC (n.d.), *Equipment Authorization Procedures*, https://www.fcc.gov/general/equipment-authorization-procedures (accessed on 16 March 2022). [196]

FCC CSRIC VIII (2022), *Report on Challenges to the development of ORAN technology and recommendations on how to overcome them*, FCC, https://www.fcc.gov/file/24520/download. [132]

Fierce Telecom (2021), *Lumen taps into Azure ecosystem with Microsoft edge deal*, https://www.fiercetelecom.com/telecom/lumen-taps-into-azure-ecosystem-microsoft-edge-deal?mkt_tok=Mjk0LU1RRi0wNTYAAAF-IS37ay7unF0D66q3CRRN-faeGJUeCCcH07ZhyU2kOTz3iC3AP07-kaj2M70PRSOfZewu7lgEK4Ghy5svv1aNR_F74F9Ates0sUoKVDuEy7vWdzUSwY0. [70]

FireEye (2020), *SolarWinds*, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. [17]

First Point (2020), *A Step by Step Guide to SS7 Attacks*, https://www.firstpoint-mg.com/blog/ss7-attack-guide. [155]

Forbes (2020), *5 Key Security Lessons from the Cloud Hopper Mega Hack*, https://www.forbes.com/sites/martingiles/2020/01/03/cloud-computing-security-cloud-hopper/. [95]

Forbes (2020), “Orange, Europe’s fourth largest mobile operator, confirms ransomware attack”, https://www.forbes.com/sites/daveywinder/2020/07/17/orange-europes-fourth-largest-mobile-operator-confirms-ransomware-attack-nefilim-data-theft/?sh=14e84aee4780. [33]

France (2019), *Code des postes et des communications électroniques [Post and Electronic Communications Code]*, Légifrance, https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070987. [210]

France (2019), *Code pénal {Penal Code]*, Légifrance, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165405/. [209]

FRRouting (2021), *FRRouting Project*, Linux Foundation Collaborative Projects, https://frrouting.org/ (accessed on 10 March 2022). [105]

Fujitsu (2020), *Fact Sheet: 5G Open RAN System Integration*, https://marketing.us.fujitsu.com/rs/407-MTR-501/images/5G%20ORAN%20System%20Integration%20FS%20Final.pdf (accessed on 11 February 2022). [118]

G7 (2021), *Digital and Technology Ministerial Declaration*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/981567/G7_Digital_and_Technology_Ministerial_Declaration.pdf. [191]

G7 (2021), *Framework for G7 Collaboration on Digital Technical Standards*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986159/Annex_1__Framework_for_G7_collaboration_on_Digital_Technical_Standards. [192]

pdf.

Google Cloud (2020), *AT&T and Google Cloud team up to enable network edge 5G computing solutions for enterprises*, https://cloud.google.com/press-releases/2020/0305/google-cloud-att-collaboration. [64]

Google Cloud (2020), *Google Cloud unveils strategy for telecommunications industry*, https://cloud.google.com/blog/topics/inside-google-cloud/google-cloud-unveils-strategy-telecommunications-industry. [61]

Google Cloud (2020), *Orange and Google Cloud to Form Strategic Partnership in Data, AI and Edge Computing Services*, Orange Business, https://www.orange-business.com/en/press/orange-and-google-cloud-form-strategic-partnership-data-ai-and-edge-computing-services. [72]

Government of Brazil (2020), *INSTRUÇÃO NORMATIVA Nº 4, DE 26 DE MARÇO DE 2020 [Normative Instruction No. 4]*, https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-250059468 (accessed on 10 March 2022). [197]

Government of Ireland (2021), *Cyber attack on HSE systems*, https://www.gov.ie/en/news/ebbb8-cyber-attack-on-hse-systems/. [3]

GSMA (2021), *Open and virtualised radio access networks: An explanatory guide for policymakers*, GSMA, https://www.gsma.com/publicpolicy/wp-content/uploads/2021/02/GSMA_Open_and_Virtualised_Radio_Access_Networks_An_Explanatory_Guide_for_Policymakers.pdf. [109]

GSMA (2019), *Dr Lauren: AI-based network failure Root Cause Analysis solution*, https://www.gsma.com/futurenetworks/wiki/ai-based-network-failure-root-cause-analysis-solution-kt/ (accessed on 10 December 2020). [147]

GSMA (2019), *SKT Tango: AI-assisted Network Operation System*, https://www.gsma.com/futurenetworks/wiki/case-study-skt/. [146]

Hacker News (2020), *Amnesia:33 — Critical TCP/IP Flaws Affect Millions of IoT Devices*, https://thehackernews.com/2020/12/amnesia33-critical-tcpip-flaws-affect.html. [40]

IBM (2021), *Laying a foundation for innovation with Telefónica*, https://newsroom.ibm.com/Laying-a-foundation-for-innovation-with-Telefonica. [74]

IBM (2021), *Network slicing at the edge*, https://www.ibm.com/cloud/blog/network-slicing-at-the-edge. [50]

IBM (2020), *An IBM-AT&T Collaboration to bring hybrid cloud to enterprise 5G*, https://newsroom.ibm.com/An-IBM-AT-T-Collaboration-to-Bring-Hybrid-Cloud-to-Enterprise-5G. [66]

IBM Cloud (2021), *Containers vs. Virtual Machines (VWs): What's the difference?*, https://www.ibm.com/cloud/blog/containers-vs-vms. [43]

IMDA (2021), *Infocomm Media Cyber Security*, https://www.imda.gov.sg/regulations-and-licensing-listing/infocomm-media-cyber-security (accessed on 21 February 2022). [229]

IMDA (2021), *Next wave of 5G growth and deployment in Singapore: Policy and regulatory design for 2.1 GHz band*, https://www.imda.gov.sg/-/media/Imda/Files/Regulations-and- [200]

Licensing/Regulations/Consultations/2021/Next-Wave-of-5G-Growth-and-Deployment-in-Singapore/IMDA-Decision--21-GHz-Policy-and-Regulatory-Framework.pdf?la=en&hash=F6858B0C7251B64AFF5E3B95688C47ED (accessed on 4 October 2021).

ITU (2015), *Recommendation ITU-R M.2083-0: IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*, ITU, https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf. [52]

Juniper (2020), *What is multi-access edge computing?*, https://www.juniper.net/us/en/research-topics/what-is-multi-access-edge-computing.html. [84]

Kaspersky (n.d.), *Global Transparency Initiative*, https://www.kaspersky.com/transparency-center. [187]

Koonin, L. et al. (2020), *Trends in the Use of Telehealth During the Emergence of the COVID-19 Pandemic — United States, January-March 2020*, pp. 1595-1599, http://dx.doi.org/10.15585/mmwr.mm6943a3. [26]

KT (2021), *KT, '5G 단독모드(SA)' 상용화 [KT commercializes '5G exclusive mode (SA)']*, KT, https://corp.kt.com/html/promote/news/report_detail.html?hash=3&rows=10&page=1&datNo=16610. [56]

Linux Foundation (2022), *LFX Security: Instill trust with complete code security*, https://lfx.linuxfoundation.org/tools/security. [182]

Linux Foundation (2020), *Annual report 2020*, https://linuxfoundation.org/wp-content/uploads/2020-Linux-Foundation-Annual-Report_120520.pdf. [183]

LRT (2022), *Lithuania's state-owned energy group hit by 'biggest cyber attack in a decade'*, https://www.lrt.lt/en/news-in-english/19/1736266/lithuania-s-state-owned-energy-group-hit-by-biggest-cyber-attack-in-a-decade. [6]

MIC (2021), *「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」（案）に対する意見募集の結果及び「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」の公表*, https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html. [170]

MIC (2020), *Information and Communications in Japan 2020*, https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2020/chapter-1.pdf#page=5. [220]

Microsoft (2023), *Transparency Centers*, https://docs.microsoft.com/en-us/security/gsp/contenttransparencycenters. [185]

Microsoft (2023), *What are the Microsoft SDL practices*, https://www.microsoft.com/en-us/securityengineering/sdl/practices (accessed on 2022). [164]

Microsoft (2021), *AT&T to run its mobility network on Microsofts Azure for Operators Cloud, delivering cost efficient 5G Services at scale*, https://news.microsoft.com/2021/06/30/att-to-run-its-mobility-network-on-microsofts-azure-for-operators-cloud-delivering-cost-efficient-5g-services-at-scale/. [79]

Microsoft (2021), *Protecting on-premises Exchange Servers against recent attacks*, https://www.microsoft.com/security/blog/2021/03/12/protecting-on-premises-exchange- [157]

servers-against-recent-attacks/.

Microsoft (2019), *AT&T and Microsoft announce a strategic alliance to deliver innovation with cloud, AI and 5G*, https://news.microsoft.com/2019/07/17/att-and-microsoft-announce-a-strategic-alliance-to-deliver-innovation-with-cloud-ai-and-5g/. [67]

Microsoft Azure (2020), *Microsoft partners with the telecommunications industry to roll out 5G and more*, Microsoft Azure, https://azure.microsoft.com/en-us/blog/microsoft-partners-with-the-telecommunications-industry-to-roll-out-5g-and-more/. [60]

Mobile World Live (2021), *When will we see 5G network slicing in the US?*, https://www.mobileworldlive.com/blog/blog-when-will-we-see-5g-network-slicing-in-the-us. [57]

National Cyber and Information Security Agency (NÚKIB) (2021), *Prague 5G Security Conference 2021*, https://www.nukib.cz/en/infoservis-en/news/1775-5g-security-conference-2021/ (accessed on 14 February 2022). [119]

NBC News (2021), *50,000 security disasters waiting to happen: The problem of America's water supplies*, https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206. [29]

NEC (2021), *5 Key Lessons from Integrating and Deploying Open RAN*, https://www.nec.com/en/global/solutions/5g/Blog_5_Key_Lessons_from_Integrating_and_Deploying_Open_RAN.html (accessed on 11 February 2022). [117]

NIS Cooperation Group (2022), *Report on the cybersecurity of Open RAN*, https://ec.europa.eu/newsroom/dae/redirection/document/86603 (accessed on 20 June 2022). [115]

NIS Cooperation Group (2019), *EU coordinated risk assessment of the cybersecurity of 5G networks*, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132. [38]

NIS Cooperation Group (EU) (2020), *EU Toolbox of risk mitigating measures - Cybersecurity of 5G networks*, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures. [18]

NIST (2023), *Cybersecurity Framework*, https://www.nist.gov/cyberframework. [171]

NIST (2023), *Updating the NIST Cybersecurity Framework – Journey To CSF 2.0*, NIST, https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20. [173]

NIST (2020), *NIST Special Publication 800-207: Zero Trust Architecture*, https://doi.org/10.6028/NIST.SP.800-207. [167]

NIST (2018), *NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. [161]

NL Times (2021), *Huawei was able to eavesdrop on Dutch mobile network KPN: Report*, https://nltimes.nl/2021/04/17/huawei-able-eavesdrop-dutch-mobile-network-kpn-report. [169]

Nokia (2023), *Software-defined access networks*, https://www.nokia.com/networks/solutions/software-defined-access-networks/. [48]

Nokia (n.d.), *Fixed access network slicing*, https://www.nokia.com/networks/solutions/fixed-access-network- [232]

slicing/#:~:text=Capture%20new%20opportunities%20with%20the%20Network%20as%20a%20Service.&text=Virtual%20slices%20of%20the%20fixed,converged%20operator)%20or%20third%20parties.

Nomios (2023), *What is White Box Switching?*, https://www.infradata.com/resources/white-box-switching/ (accessed on 28 September 2021). [98]

NSA/CISA (2022), *Open Radio Access Network Security Considerations*, https://www.cisa.gov/sites/default/files/publications/open-radio-access-network-security-considerations_508.pdf (accessed on 19 September 2022). [131]

NTIA (2021), *SBOM at a glance*, https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf. [188]

NTIA (2020), *CSCRIP*, https://www.ntia.doc.gov/cscrip. [179]

NTT (2019), *NTT and Microsoft form a strategic alliance to enable new digital solutions*, https://hello.global.ntt/en-us/newsroom/ntt-microsoft-form-strategic-alliance-enabling-new-digital-solutions. [71]

NVIDIA (2020), *Lenovo and NVIDIA Spark New Era of Open Networking*, NVIDIA, https://blogs.nvidia.com/blog/2020/09/15/lenovo-open-networking/ (accessed on 28 September 2021). [102]

NVIDIA (2020), *Programming the Modern Data Center: Cumulus Joins NVIDIA's Networking Group*, https://blogs.nvidia.com/blog/2020/06/16/cumulus-programming-networks/ (accessed on 29 September 2021). [101]

OECD (2023), *Broadband Portal*, https://www.oecd.org/sti/broadband/broadband-statistics/ (accessed on March 2022). [24]

OECD (2022), *Broadband networks of the future*, OECD Publishing, https://doi.org/10.1787/755e2d0c-en (accessed on August 2022). [23]

OECD (2021), *Encouraging vulnerability treatment: overview for policy makers*, OECD Publishing, Paris, https://doi.org/10.1787/20716826. [14]

OECD (2021), *Enhancing the digital security of products: a policy discussion*, https://doi.org/10.1787/20716826. [135]

OECD (2021), *OECD-G7 Report on Fostering Economic Resilience in a World of Open and Integrated Markets*, https://www.oecd.org/newsroom/OECD-G7-Report-Fostering-Economic-Resilience-in-a-World-of-Open-and-Integrated-Markets.pdf. [1]

OECD (2021), *Smart policies for smart products: a policymaker's guide to enhancing the digital security of products*, https://www.oecd.org/digital/smart-policies-for-smart-products.pdf. [91]

OECD (2021), *Understanding the digital security of products*, https://doi.org/10.1787/abea0b69-en. [8]

OECD (2020), *Dealing with digital security risk during the Coronavirus (COVID-19) crisis*, https://www.oecd.org/coronavirus/policy-responses/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis-c9d3fe8e/. [15]

OECD (2020), *Keeping the Internet up and running in times of crisis*, [22]

http://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/.

OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en. [154]

OECD (2019), "Policies for the protection of critical information infrastructure: Ten years later", *OECD Digital Economy Papers*, No. 275, OECD Publishing, Paris, https://dx.doi.org/10.1787/efb55c54-en. [134]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*, OECD Legal Compendium, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [141]

OECD (2019), *Recommendation of the Council on Digital Security of Critical Activities*, OECD Legal Compendium, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456. [162]

OECD (2019), "The road to 5G networks: Experience to date and future developments", *OECD Digital Economy Papers*, No. 284, OECD Publishing, Paris, https://dx.doi.org/10.1787/2f880843-en. [20]

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264245471-en. [163]

OECD (2014), "Cloud Computing: The Concept, Impacts and the Role of Government Policy", *OECD Digital Economy Papers*, No. 240, OECD Publishing, Paris, https://dx.doi.org/10.1787/5jxzf4lcc7f5-en. [58]

Ofcom (2023), *Our network security and network resiliency work*, https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work (accessed on 21 February 2022). [195]

ONAP (2022), *ONAP Kohn Release is Now Available*, ONAP, https://www.onap.org/blog/2022/12/13/onap-kohn-release-is-now-available. [216]

Open Compute Project (2021), *Networking*, https://www.opencompute.org/projects/networking. [99]

Open Network Automation Platform (ONAP) (2023), *Home*, https://www.onap.org/. [215]

Open Networking Foundation (2021), *Our Mission*, https://opennetworking.org/mission/. [97]

Open Source Initiative (2007), *The Open Source Definition*, https://opensource.org/osd. [211]

OpenSSF (2023), *Open Source Security Foundation (OpenSSF)*, https://openssf.org/. [181]

Oracle (2021), *Telefonica España and Oracle Announce Collaboration to Accelerate Cloud Adoption*, https://www.oracle.com/news/announcement/telefonica-and-oracle-announce-collaboration-to-accelerate-cloud-adoption-2021-09-27/. [83]

O-RAN Alliance (2023), *Open Software for the RAN*, https://www.o-ran.org/software. [114]

O-RAN Alliance (2022), *O-RAN Alliance Introduces 40 New Specifications Released Since November 2021*, O-RAN Alliance, https://www.o-ran.org/blog/o-ran-alliance-introduces-40-new-specifications-released-since-november-2021 (accessed on 21 June 2022). [139]

O-RAN Alliance (2020), *O-RAN ALLIANCE*, https://www.o-ran.org/ (accessed on [149]

14 December 2020).

O-RAN Alliance (2020), *O-RAN Use Cases and Deployment Scenarios Towards Open and Smart RAN*. [150]

O-RAN Alliance (2020), *The O-RAN Alliance and the Telecom Infra Project (TIP) reach new level of collaboration for open radio access networks*, https://www.o-ran.org/press-releases/the-o-ran-alliance-and-the-telecom-infra-project-tip-reach-new-level-of-collaboration-for-open-radio-access-networks (accessed on 4 October 2021). [113]

O-RAN Alliance (2018), *O-RAN: Towards an Open and SmartRAN*, https://assets-global.website-files.com/60b4ffd4ca081979751b5ed2/60e5afb502810a0947b3b9d0_O-RAN%2BWP%2BFInal%2B181017.pdf. [112]

OSS Watch (2013), *Governance models*, http://oss-watch.ac.uk/resources/governancemodels (accessed on 30 September 2021). [212]

Parliament of Australia (2022), *Improved reforms to counter espionage, foreign interference in telecommunications sector*, https://www.aph.gov.au/About_Parliament/House_of_Representatives/About_the_House_News/Media_Releases/Improved_reforms_to_counter_espionage_foreign_interference_in_telecommunications_sector (accessed on 5 October 2021). [204]

Parliament of Australia (2021), *Security Legislation Amendment (Critical infrastructure) Bill, 2021: revised explanatory memorandum*, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6657_ems_c345cb8e-87b2-461a-87f9-53d9aad3afc6/upload_pdf/JC003855_Revised%20Explanatory%20Memorandum.pdf;fileType=application%2Fpdf (accessed on 21 February 2022). [207]

Positive Technologies (2019), *Telecom Security in the Era of 5G and IoT*, https://www.slideshare.net/PositiveTechnologies/telecom-security-in-the-era-of-5g-and-iot. [92]

Positive Technologies (2018), *SS7 vulnerabilities and attack exposure report*, GSMA, https://www.gsma.com/membership/wp-content/uploads/2018/07/SS7_Vulnerability_2017_A4.ENG_.0003.03.pdf. [156]

PwC (2017), *Operation Cloud Hopper*, https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf. [96]

Quad Critical and Emerging Technology Working Group (2023), *Open RAN security report*, Ministry of Internal Affairs and Communications of Japan, https://www.soumu.go.jp/main_content/000881591.pdf. [133]

Rakuten (2022), *Rakuten Mobile 4G service covers 96% of Japan's population – four years ahead of schedule*, https://rakuten.today/blog/rakuten-mobile-4g-service-covers-96-japans-population.html (accessed on 14 February 2022). [125]

Rakuten (2021), *1&1 and Rakuten agree far-reaching partnership to build Europe's first fully virtualized mobile network based on new OpenRAN technology*, https://corp.rakuten.eu/pressrelease/11-and-rakuten-agree-far-reaching-partnership-to-build-europes-first-fully-virtualized-mobile-network-based-on-new-openran-technology/ (accessed on 12 February 2022). [127]

Rakuten Mobile (2020), *Rakuten Mobile and NEC begin production of Open RAN 5G radio equipment*, https://corp.mobile.rakuten.co.jp/english/news/press/2020/0324_01/ (accessed on 4 October 2021). [124]

RedHat (2018), *What's the difference between cloud and virtualization?*, https://www.redhat.com/en/topics/cloud-computing/cloud-vs-virtualization. [59]

Reserve Bank of New Zealand (2022), *Our response to the data breach*, https://www.rbnz.govt.nz/about-us/responsibility-and-accountability/our-response-to-the-data-breach. [4]

SC Magazine (2004), *Jericho Forum brings its deperimeterization concept to US*, SC Magazine, https://www.scmagazine.com/news/-/jericho-forum-brings-its-deperimeterization-concept-to-u-s. [165]

Schneier, B. (1999), *A Plea for Simplicity. You can't secure what you don't understand.*, Schneier on security, https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html. [137]

SDX Central (2020), *Telefónica Germany Taps AWS for 5G Core Virtualization*, https://www.sdxcentral.com/articles/news/telefonica-germany-taps-aws-for-5g-core-virtualization/2020/09/. [82]

SDxCentral Studios (2016), *What is Software Defined Networking (SDN)? Definition*, https://www.sdxcentral.com/networking/sdn/definitions/what-the-definition-of-software-defined-networking-sdn/. [45]

Security Boulevard (2021), *How a DDoS Attack on an Internet Service Provider Can Paralyze Critical Infrastructure*, https://securityboulevard.com/2021/05/how-a-ddos-attack-on-an-internet-service-provider-can-paralyze-critical-infrastructure/. [12]

Siriwardhana, Y. et al. (2021), *AI and 6G Security: Opportunities and Challenges*, Porto, Portugal, https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482503. [153]

SolarWinds Corp. (2020), *Form 8-K Solarwinds Corporation, Current Report, December 14, 2020*, SolarWinds Corp., https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/57108215-4458-4dd8-a5bf-55bd5e34d451.pdf. [93]

Subedi, P. et al. (2021), *Network slicing: a next generation 5G perspective*, J Wireless Com Network, https://doi.org/10.1186/s13638-021-01983-7. [53]

Synopsys (2023), *2023 Open Source Security and Risk Analysis Report*, Synopsys, https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html# (accessed on 10 March 2022). [213]

Tech Times (2021), *Germany's €300 million Open RAN push sets tone for European debate*, https://www.techtimes.com/articles/257325/20210222/germany-s-%E2%82%AC300-million-open-ran-push-sets-tone-for-european-debate.htm (accessed on 4 October 2021). [221]

Techcrunch (2019), *Huuawei opens a cybersecurity transparency center in the heart of europe*, https://techcrunch.com/2019/03/06/huawei-opens-a-cybersecurity-transparency-center-in-the-heart-of-europe/. [184]

TechTarget (2022), *Open networking*, TechTarget, https://www.techtarget.com/searchnetworking/definition/open-networking (accessed on [104]

29 September 2021).

Telecom Infra Project (2023), *OpenRAN*, https://telecominfraproject.com/openran/ (accessed on 4 October 2021). [111]

Telecom Infra Project (n.d.), *Home: A new approach to building and depoying telecom network infrastructure*, https://telecominfraproject.com/ (accessed on 4 October 2021). [110]

Telecommunications Authorization Act (2022), *47 USC 906*, https://uscode.house.gov/view.xhtml?path=/prelim@title47/chapter8&edition=prelim. [219]

Telefonica (2021), *Hello! I am Aura, the Artificial Intelligence of Telefónica*, https://aura.telefonica.com/ (accessed on 28 September 2021). [145]

Telefónica (2021), *Cisco, Telefónica y la Universidade de Vigo impulsan el 'Network Slicing' sobre 5G*, https://www.telefonica.com/es/sala-comunicacion/cisco-telefonica-y-la-universidade-de-vigo-impulsan-el-network-slicing-sobre-5g/ (accessed on February 2022). [54]

Telefónica (2021), *Europe urged to act now to build Open RAN ecosystem*, https://www.telefonica.com/en/communication-room/europe-urged-to-act-now-to-build-open-ran-ecosystem/ (accessed on 11 February 2022). [123]

Telefónica Germany (2020), *Telefónica Germany/O2 builds new 5G core network in the cloud*, https://www.telefonica.de/news/press-releases-telefonica-germany/2020/09/cooperation-with-amazon-web-services-and-ericsson-drives-new-industrial-5g-solutions-telefonica-deutschland-o2-builds-its-new-5g-core-network-in-the-cloud.html. [73]

Telenet (2021), *Telenet choisit Ericsson, Nokia et Google Cloud comme partenaires pour le déploiement de son réseau 5G, moteur des innovations mobiles de demain*, https://press.telenet.be/telenet-choisit-ericsson-nokia-et-google-cloud-comme-partenaires-pour-le-deploiement-de-son-reseau-5g-moteur-des-innovations-mobiles-de-demain. [75]

The Guardian (2023), *Royal Mail resumes overseas deliveries via post offices after cyber-attack*, The Guardian, https://www.theguardian.com/business/2023/feb/21/royal-mail-international-deliveries-cyber-attack-ransom-strikes. [7]

The Independent (2021), *Hospital ransomware attack caused baby's death by shutting down heart rate display, lawsuit claims*, https://www.independent.co.uk/news/world/americas/hospital-ransomware-baby-death-lawsuit-b1930179.html. [27]

The Linux Foundation (2020), *Annual Report 2020: Advancing open collaboration amid the challenges of a lifetime*, https://www.linuxfoundation.org/resources/publications/linux-foundation-annual-report-2020. [214]

The New York Times (2020), *FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State*, https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html. [94]

The Open Group (2021), *Zero Trust Core Principles*, https://pubs.opengroup.org/security/zero-trust-principles. [166]

TIM (2021), *TIM joins the European initiative for the development of Open RAN solutions*, https://www.gruppotim.it/en/press-archive/corporate/2021/PR-TIM-ORAN-en.html (accessed on 12 February 2022). [122]

T-Mobile USA (2021), *Comments of T-Mobile USA: In the matter of Promoting the Deployment of 5G Open Radio Access Networks*, https://ecfsapi.fcc.gov/file/104280435523172/T-Mobile%20Comments%20on%20Open%20RAN%20NOI.pdf. [129]

Traficom (2021), *5G Cyber Security Hack 2021 - Safeguard the future digital society*, https://www.traficom.fi/en/news/events/5g-cyber-security-hack-2021-safeguard-future-digital-society. [177]

Traficom (2019), *5G cyber security hackaton in Finland*, https://www.traficom.fi/en/news/70-top-hackers-around-world-gathered-finland-worlds-first-open-5g-cyber-security-hackathon-was. [176]

United Kingdom (2021), *Telecommunications (Security) Act 2021*, Legislation.gov.uk, https://www.legislation.gov.uk/ukpga/2021/31/contents (accessed on 4 October 2021). [202]

US Government (2021), *Executive Order on Improving the Nation's Cybersecurity*, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. [168]

Verizon (2021), *Verizon and AWS cover 13 of top 20 metro areas with mobile edge computing*, https://www.verizon.com/about/news/verizon-aws-cover-metro-areas-mec. [77]

Vitard, A. (2021), *Le service d'assainissement des eaux d'Oloron-Sainte-Marie a été pris pour cible par des hackers*, L'Usine digitale, https://www.usine-digitale.fr/article/le-service-d-assainissement-des-eaux-d-oloron-sainte-marie-a-ete-pris-pour-cible-par-des-hackers.N1145927. [30]

VMWare (2021), *Vodafone selects VMware for automation and orchestration of all workloads running on core networks across Europe*, https://news.vmware.com/releases/vodafone-and-vmware. [49]

VMware (2023), *What is network virtualization?*, https://www.vmware.com/topics/glossary/content/network-virtualization.html (accessed on 9 February 2022). [42]

VMware (2020), *Containerized Network Functions on Virtual Machines or Bare Metal? Securing, Managing and Optimizing CNFs and 5G services at scale*, https://telco.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/microsites/telco/vmw-telco-cnf-on-vm-or-bare-metal-whitepaper.pdf (accessed on 9 February 2022). [44]

Vodafone (2023), *How to contact us: What can TOBi do?*, https://www.vodafone.co.uk/help-and-information/introducing-tobi (accessed on 28 September 2021). [144]

Vodafone (2022), *Vodafone switches on UK's first 5G Open RAN site*, https://www.vodafone.com/news/technology/5g-open-ran-first-uk-site (accessed on 14 February 2022). [228]

Vodafone (2021), *Vodafone and Google Cloud to develop industry-first global data platform*, https://www.vodafone.com/news/services/vodafone-google-cloud-industry-first-global-data-platform. [78]

Vodafone (2021), *Vodafone And Nokia Develop Machine Learning System To Detect Mobile Network Anomalies*, https://www.vodafone.com/news/press-release/vodafone-nokia-partnership (accessed on 9 August 2021). [148]

Vodafone (2021), *Vodafone selects key partners to build Europe's first commercial Open RAN network*, https://www.vodafone.com/news/corporate-and-financial/vodafone-europe-first-commercial-open-ran-network (accessed on 14 February 2022). [227]

Vodafone (2021), *World first: UK Power Networks to use Vodafone 5G in smart substations*, https://newscentre.vodafone.co.uk/press-release/5g-for-uk-power-networks-world-first-smart-substation-trial/?utm_source=ukpnAndrea (accessed on 28 July 2021). [55]

White House (2023), *National Cybersecurity Strategy*, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. [189]

White House (2021), *Executive Order on Improving the Nation's Cybersecurity*, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. [10]

White House (2021), *Fact Sheet: Quad Leaders' Summit*, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/ (accessed on February 2022). [224]

White House (2021), *Fact Sheet: U.S.-Japan Competitiveness and Resilience (CoRe) Partnership*, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/fact-sheet-u-s-japan-competitiveness-and-resilience-core-partnership/ (accessed on 15 February 2022). [225]

White House (2021), *Joint Statement from Quad Leaders*, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/joint-statement-from-quad-leaders/ (accessed on 15 February 2022). [223]

White House (2021), *Statement by NSC Spokesperson Emily Horne on U.S. Support for the Third Annual Prague 5G Security Conference*, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/02/statement-by-nsc-spokesperson-emily-horne-on-u-s-support-for-the-third-annual-prague-5g-security-conference/ (accessed on 14 February 2022). [121]

White House (2021), *U.S.-ROK Leaders' Joint Statement*, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/21/u-s-rok-leaders-joint-statement/ (accessed on 15 February 2022). [226]

Wired (2019), *Decades-Old Code Is Putting Millions of Critical Devices at Risk*, https://www.wired.com/story/urgent-11-ipnet-vulnerable-devices/. [41]

Wired (2016), *Inside the cunning, unprecedented hack of Ukraine's power grid*, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. [31]

ZDNet (2021), *Colonial Pipeline attack: Everything you need to know*, https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/. [2]

ZDNet (2020), *Ransomware gang demands $7.5 million from Argentinian ISP*, https://www.zdnet.com/article/ransomware-gang-demands-7-5-million-from-argentinian-isp/. [32]

Notes

[1] See the accompanying OECD reports on *Routing Security: BGP incidents, mitigation techniques and policy actions* (https://doi.org/10.1787/40be69c8-en) and *Security of the Domain Name System (DNS): an introduction for policy makers* (https://doi.org/10.1787/285d7875-en) for further discussion on key digital security regarding communication networks' protocols.

[2] Approaches that excessively focus on national security even tend to confuse threats and vulnerabilities, and often suggest for instance that vulnerabilities only exist because of threats (e.g. conflating all vulnerabilities with those ones inserted intentionally in a product's code).

[3] For further detail on various cloud services, please see the OECD report, *Broadband Networks of the Future* (2022[23]).

[4] Figures consider levels in September – December 2019 to be "pre-pandemic", compared to levels in the first quarter of 2020 (e.g., March 2020).

[5] However, this may evolve in the future as innovations in Wi-Fi emerge (e.g., early discussions of the next Wi-Fi standard (Wi-Fi 7) include goals to provide the reliability required to support mission-critical applications).

[6] Cyber dependencies in critical infrastructure are further discussed in (OECD, 2019[138]).

[7] A network function is a functional building block within a network infrastructure, which has well-defined external interfaces and a well-defined functional behaviour (ETSI, 2020[243]).

[8] Each VM contains a "virtual copy of the hardware that the OS [operating system] requires to run an application and its associated libraries and dependencies" (IBM Cloud, 2021[44]).

[9] Containers are self-contained packages that have everything needed to run one application or microservice (e.g., application, its libraries and any dependencies), which run on top of a host operating system and can be run in a variety of environments (e.g., the cloud, traditional IT infrastructure) (IBM Cloud, 2021[44]). Containers also enable the deployment of microservices, which is also growing in popularity to scale applications. As the name implies, a microservice is a small task, one of several tasks or actions required to deliver an application or service. One container can host one or several microservices, depending on the needs and decisions of the network operator.

[10] For example, a network may use VMs to virtualise their hardware due to the benefits in terms of isolation from other VMs, while at the same time using containers for their applications to use a VM's resources more effectively (VMware, 2020[45]).

[11] While important for 5G networks in particular, network slicing as a technology could be applied to fixed networks as well. For instance, slices of fixed network infrastructure could be tailored to meet the requirements of different customers to meet different needs (e.g., a slice for business subscribers, residential subscribers, mobile backhaul for 3G, 4G, and 5G, respectively) (Nokia, n.d.[243]).

[12] A "substation" is a part of the system of electrical generation, transmission, and distribution that transforms energy.

[13] Near edge compute can usually deliver low latency (e.g., under 75 millisecond (ms) (Dell Technologies, 2021[240]) and host services such as caches of content delivery networks (CDNs) (Accenture and Intel, 2021[240]). Closer to the end user, far edge compute can support lower latency (e.g., <20 ms), serving applications requiring ultra-low latency and high bandwidth (Dell Technologies, 2021[240]). In order to be closer to the end users, far edge compute nodes may be deployed at the premise of an enterprise customer, or in a street cabinet or wireless base station, (Accenture and Intel, 2021[240]), and they may be placed in more remote and less protected locations, requiring a different level of security and resiliency at the hardware/firmware levels.

[14] It should be noted however that the dichotomy between "hardware" and "software" is not absolute, as hardware products contain code, often referred to as "firmware". Firmware also contains vulnerabilities, which may be exploited by malicious actors (e.g. the Meltdown and Spectre vulnerabilities in microprocessors, see (OECD, 2021[8])).

[15] Please see the OECD report, *Broadband Networks of the Future* for more technical descriptions of virtualised RAN and open RAN (2022[23]).

[16] For example, Deutsche Telekom piloted an Open RAN town in Neubrandenburg and published a report on its findings (Deutsche Telekom AG, 2023[244]).

[17] However, increased competition does not necessarily result in an enhanced level of digital security. In fact, many other factors can be used by competitors to differentiate their products, including price, usability and performance. Competition should therefore be understood as one important but insufficient ingredient to enhance digital security risk management. Other key ingredients include transparency and requirements resulting in an enhanced duty of care for suppliers (OECD, 2021[8]).

[18] The Going Digital Toolkit Note on Enhancing Digital Security of Critical Activities provides an overview of the policy framework recommended by the OECD, illustrated by measures taken in some OECD countries (Bernat, 2021[163])

[19] An exchange rate of 0.811 GBP/USD for the year 2022 from OECD.stat (https://data.oecd.org/conversion/exchange-rates.htm) has been used.

[20] An exchange rate of 0.811 GBP/USD for the year 2022 from OECD.stat (https://data.oecd.org/conversion/exchange-rates.htm) has been used.

[21] An exchange rate of 0.950 EUR/USD (Germany) for the year 2022 from OECD.stat (https://data.oecd.org/conversion/exchange-rates.htm) has been used.

[22] An exchange rate of 0.950 EUR/USD (Germany) for the year 2022 from OECD.stat (https://data.oecd.org/conversion/exchange-rates.htm) has been used.

[23] Each project focuses on a different aspect, such as reducing capabilities based on application needs, using AI for network automation, or using sub-terahertz frequencies for joint communication and sensing technologies.

[24] The Heartbleed vulnerability was discovered in Open SSL (Secure Sockets Layer), an open-source cryptography library used to implement the TLS (Transport Layer Security) protocol in web servers and applications. The vulnerability allowed theft of the servers' private keys and users' session cookies and passwords. Open SSL is widely used across the Internet: at the time of disclosure, about 17% of the Internet's web servers using SSL certificates were considered vulnerable.

[25] 3GPP brings together the Association of Radio Industries and Businesses (ARIB), the Alliance for Telecommunications Industry Solutions (ATIS), the China Communications Standards Association (CCSA), the European Telecommunications Standards Institute (ETSI), the Telecommunications Standards Development Society India (TSDSI), the Telecommunication Technology Association (TTA) and the Telecommunication Technology Committee (TTC). For more information, see https://www.3gpp.org/about-3gpp/partners.

[26] An exchange rate of 0.811 GBP/USD for the year 2022 from OECD.stat (https://data.oecd.org/conversion/exchange-rates.htm) has been used.

[27] An exchange rate of 0.950 EUR/USD (Germany) for the year 2022 from OECD.stat (https://data.oecd.org/conversion/exchange-rates.htm) has been used.