# 5G cybersecurity

**Study period 2022-2025**

**Question 3/2**

*Securing information and communication networks: Best practices for developing a culture of cybersecurity*

**Interim deliverable 2024**

## Executive summary

This interim deliverable emphasizes key aspects of 5G cybersecurity given the rise in global cyberthreats and the critical nature of telecommunications infrastructure. With its advanced software, cloud-based architecture, and extensive connectivity, 5G technology introduces **new security paradigms**. It offers significant benefits but also brings new risks, necessitating robust cybersecurity measures to protect against threats.

The complexity of 5G networks demands advanced security strategies and collaboration among different stakeholders. **Standards development organizations** (SDOs) have begun to standardize cybersecurity aspects of 5G networks, but continuous cooperation and communication are necessary to avoid duplication of efforts.

**Proactive cybersecurity measures** are crucial at all stages of network deployment, with vendors and operators having responsibilities in managing cybersecurity risks.

**A variety of national policies and regulations for 5G** cybersecurity are being developed. Many countries have already adopted their approaches to mitigate security risks and are now focusing on their implementation and compliance regimes.

**Investing in education and training** is vital to address the growing demand for skilled cybersecurity professionals.

Looking ahead, **planning for 6G** emphasizes enhanced cybersecurity and resilience from the outset. ITU's IMT-2030 framework reflects a commitment to integrating robust security measures to support future technological advancements.

# Introduction

The terms of reference for Question 3/2 of ITU-D Study Group 2, "Securing information and communication networks: Best practices for developing a culture of cybersecurity", were reviewed at the most recent World Telecommunication Development Conference, held in Kigali, Rwanda, in June 2022. One of the specific issues identified for study was to "discuss challenges and approaches for 5G cybersecurity".

The approved terms of reference for Question 3/2 recognize that cybersecurity threats continue to be a major concern for governments, organizations and individuals worldwide. Globally, cyber insecurity is ranked as the fourth most severe short-term risk, according to the Global Risks Report 2024 from the World Economic Forum[1]. Telecommunications networks, which in many jurisdictions are considered a vital component of critical national infrastructure or essential services, are vulnerable to cyberattacks, which can disrupt essential services and public safety.

The introduction of 5G technology represents a significant change in telecommunications, offering faster speeds and better connectivity with the potential to improve industries, expand Internet of Things (IoT) applications, and bring new approaches to digital communication. However, the sophisticated architecture that enables these advances brings with it complex cybersecurity challenges that require comprehensive understanding and robust protective measures.

Recognizing the critical importance of safeguarding 5G infrastructure and services, Study Group 2 working on Question 3/2 organized a dedicated full-day workshop on 2 May 2024 that brought together policymakers, regulators, operators and other members of the telecommunication industry to discuss the complexities of 5G cybersecurity, share existing practices, and explore innovative solutions to emerging threats. As 5G networks are deployed globally, establishing a secure ecosystem is imperative to ensure the integrity, availability, and confidentiality of information, as well as to protect the infrastructure that has become the backbone of the digital economy.

This report reflects the discussions from the workshop as well as contributions received during this study cycle. It is not intended to be a technical report about 5G cybersecurity; rather, the goal is to share reflections and good practices gathered in the context of the study question that the ITU Membership can consider and implement in their national contexts. The focus of this report is primarily on 5G cybersecurity of public electronic networks.

## 1. 5G brings new security paradigms for telecoms networks

### *Overview of 5G cybersecurity*

5G is characterized by its advanced software systems that enable more flexible configuration and massive connectivity of subscribers and devices. This technology supports low-latency applications, such as augmented reality, telesurgery, and integrated Internet services, which rely on a robust and reliable network. One of the primary use cases of 5G is the Internet of Things (IoT), which capitalizes on 5G's ability to connect a vast number of endpoints. 5G technology is poised to revolutionize connectivity, and this also presents new and dynamic cybersecurity risks and challenges.

In a break with previous generations of wireless technologies, 5G introduces a significant shift towards cloud-based architecture, software-defined networks (SDN) and network function virtualization (NFV). This shift creates a more complex and dynamic cybersecurity landscape.

As 5G becomes more widespread, the telecommunication infrastructure is expected to become an even more attractive target for malicious cyber activity necessitating advanced security measures that can adapt to evolving threats. Cybersecurity for 5G should focus on increasing the resilience of the entire ecosystem, including the infrastructure and applications. This includes protecting connected devices, data, and networks from cyberthreats.

Recognizing that different organizations use different definitions of cybersecurity[2], it should be borne in mind that the term "5G cybersecurity" in this report refers to cybersecurity in the context of 5G, with its new parameters, standards, and technology features, which need to be properly managed to safeguard the whole digital ecosystem and ensure cyber resilience.

> At ITU cybersecurity is defined in Recommendation X.1205 of the Telecommunication Standardization Sector (ITU-T) as "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:*
>
> - *Availability*
> - *Integrity, which may include authenticity and non-repudiation*
> - *Confidentiality.*"[3]

### *Legacy network deployments*

Operators initially tend to deploy 5G networks on a non-standalone (NSA) basis, leveraging existing 4G infrastructure before deploying a standalone (SA)

[1] Global Risks Report 2024

[2] https://www.enisa.europa.eu/publications/definition-of-cybersecurity

[3] https://www.itu.int/rec/T-REC-X.1205-200804-I

end-to-end 5G network[4]. 5G NSA networks inherit the legacy vulnerabilities of 4G, or even 2G/3G, which need to be managed accordingly. For some operators, this equates to a "technical debt": managing older systems means that a set of standardized security controls needs to be developed to measure the security status of infrastructure components at various stages of generational maturity.[5]

It is important to highlight that 5G SA presents opportunities to improve cybersecurity compared to past generations of mobile technology: it is designed to be more secure than 4G. Improvements have been noted in areas such as subscriber security and privacy, the radio access network (RAN), network core and roaming security.[6,7]

## 2. Work on standards to secure 5G is done in many SDOs, so the SDOs need to make concerted efforts to communicate and avoid duplication of work

### *SDOs active in 5G cybersecurity*

Because of the complexity of 5G technology and the issues involved, there is no one standards development organization (SDO) with an exclusive mandate for 5G cybersecurity work. To prevent duplication, mechanisms have been developed for information sharing between SDOs and for coordinating proposals and work items.

To help map these different activities and inform the direction of 5G-related security standardization work in ITU-T, Study Group 17 (SG17) prepared a technical report mapping existing standards and those under development to SDOs and their application in 5G networks.[8] The report identifies standards from ITU-T, the 3rd Generation Partnership Project (3GPP), the European Telecommunications Standards Institute (ETSI) and the Institute of Electrical and Electronics Engineers Standards Association (IEEE SA), along with non-standards resources relevant to 5G cybersecurity.

The Study Group has published 11 Recommendations on 5G security, based on submissions drafted by operators, vendors, smartphone manufacturers, content providers, and others. These focus on security in five areas: SDN-NFV, network slicing, mobile edge, 5G network management and 5G services. SG17 has established liaisons with other SDOs, such as 3GPP and the Internet Engineering Task Force (IETF), and with industry groups working on specifications having relevance for 5G cybersecurity standardization.

One such industry group is the GSM Association (GSMA). Whilst not itself a standards body, GSMA produces specifications, convening its members and engaging with SDOs to get these specifications improved and/or adopted as a standard. GSMA has published a list of baseline security controls that mobile operators can consider, on a voluntary basis, when deploying 5G networks.[9]

Given the numerous sources of information relevant to 5G security, the European Agency for Cybersecurity, ENISA, has published a unified repository of technical security controls for 5G networks, the 5G Security Controls Matrix.[10] The repository is currently published as a spreadsheet, but the agency is also developing a web tool to improve usability.

As networks become ever more complex and telecommunications converge with IP networks, it is becoming harder to attribute specific areas of standardization work to individual SDOs. This increases the risk of overlap and duplication of work, making communication and information-sharing between SDOs even more important.

### *Incorporating standards in mandatory regulatory requirements*

Standards help ensure interoperability between technologies and reduce the time needed for an innovation to reach its global market. Cybersecurity standards can define an agreed common security baseline which reflects universal good practices. Standards are the result of consensus-based processes. They can be mandatory, but in most cases they are optional, leaving vendors and operators more flexibility in their deployment decisions. In some instances, standards can become mandatory if national technical regulations incorporate a specific standard in their security requirements. National 5G cybersecurity strategies should reflect a balance between global best practices and local operational realities. As a general rule, national regulatory requirements should draw on international agreed standards, adapting them to local contexts and local needs in order to ensure the success of 5G deployment and cybersecurity of the networks.

## 3. Standards and specifications should be complemented with proactive cybersecurity measures at the different stages leading up to network deployment

### *Security considerations at the vendor level*

Standards and specifications are only one component of 5G cybersecurity. How vendors and operators implement those standards and configure them defines the security posture of 5G networks. Ericsson has adopted a holistic approach to 5G security, which is addressed at four layers: standards, vendor product development, network

[4] Devices operating on NSA 5G networks typically connect to 5G frequencies for data transmission when they need greater bandwidth and lower latency (e.g. for communication between smart cars), or to reduce the power drain on IoT-enabled devices, but continue to rely on 4G and even 2G/3G networks for voice calls and SMS messaging. Source: https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf

[5] Workshop material – Maxis

[6] https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf

[7] https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era

[8] https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-2-PDF-E.pdf

[9] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/

[10] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

deployment and network operations.[11] The company considers that such a comprehensive approach can ensure that mitigating measures are implemented a way that does justice to the interdependencies between the layers as well as the specific needs at each layer.

As a concrete example of 5G security measure, the Network Equipment Security Assurance Scheme (NESAS),[12] developed by GSMA and 3GPP, seeks to improve security levels of mobile network equipment by providing an assurance scheme that can be applied globally. The scheme is based on internal and independent expert audit – being a mixture of assessment between vendors processes and product evaluation – which offers accreditation. The aim of this scheme is to decrease the burden of security testing for network equipment providers which tend to operate at a global scale. Major vendors have already obtained NESAS accreditation. NESAS is also a candidate for the EU cybersecurity certification scheme on 5G[13] – an EU-level certification that would give conformity across the EU states. This certification would not replace the current NESAS scheme but would exist in tandem. Developing schemes/certification initiatives in such a way that they remain flexible and can be updated quickly is essential given the evolving threat landscape.

In the United Kingdom, the National Cyber Security Centre (NCSC) recommends using the vendor assessment framework,[14] guidance that helps operators assess the cyber risks associated with use of the vendor's equipment.

## *Security considerations at the operator level*

NESAS can provide a level of assurance that an item of network equipment is secure prior to deployment. As operators deploy and operate their networks, other security considerations need to be integrated, such as attack detection and automated response. This is where operators should consider leveraging AI, threat intelligence and analytics to help support their cyberdefence. 5G cybersecurity offers benefits such as real-time security and strategies such as zero trust which improve system visibility. It has its own challenges, however: maintaining connectivity across different networks with varying security levels; working with legacy components and diverse network types; and the complexities of integrating AI into security measures. Applying strict access controls according to the "least privileges" principle ensures that various rights in the network (e.g. access rights between network functions, network administrators' rights, configuration of virtualization) are minimized. A wealth of literature on the 5G-specific cybersecurity strategies is available for operators to consider.[15]

Testing of live telecoms networks is also essential for establishing the true cyber risk to telecoms networks. Operators can conduct some form of security testing against their own networks and systems, either using internal resources or by employing independent external contractors. In the United Kingdom, TBEST is an outcome-based penetration test scheme which simulates the techniques and tactics that well-resourced cyberattackers may use. It assesses how well a communications provider can detect, contain and respond to such an attack. The overall aim is to identify and address security vulnerabilities or other weaknesses in a provider's functions, processes, policies, systems or networks that could be used together to compromise a company's critical systems before detection. By undergoing the voluntary TBEST scheme, communications providers can identify specific areas in which their security could be improved, and Ofcom, the regulator, works with them to help implement appropriate changes in a timely manner.[16]

A strong business case for 5G cybersecurity is essential. While operators need to see a return on their investments in 5G services, compliance with baseline security measures should be recognized as indispensable and budgeted accordingly.

Open RAN is the disaggregation of the radio access network (RAN) and standardization of the interfaces connecting those disaggregated elements, making it possible to build networks with equipment from different vendors.

On the one hand, open RAN can bring further complexity to the telecommunications networks' supply chain. This architecture, which encourages vendor diversity in the RAN, requires further integration efforts throughout a network's supply chain which can increase the vectors of attack. On the other hand, open RAN adds transparency to supply chains, gives operators more visibility and allows them to monitor and detect security risks. In short, it improves their understanding of network architecture and equipment and makes possible more comprehensive vulnerability scanning and management. The O-RAN Alliance, the primary source of open RAN specifications, is working on security specifications for open RAN architecture and aiming to get these specifications standardized in ETSI.

NTT Docomo (Japan) is one of the operators that have embraced open RAN architecture because of its flexibility for equipment choices. The decision raised questions from a security perspective because it is generally considered that openness means that there is more opportunity for attacks. However, the operator has compared traditional RAN with open RAN and concluded there is little security difference between the two.[17]

11 https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security

12 https://www.gsma.com/solutions-and-impact/industry-services/certification-services/network-equipment-security-assurance-scheme-nesas/

13 https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

14 https://www.ncsc.gov.uk/report/vendor-security-assessment

15 See for example https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf and https://www.5gamericas.org/security-for-5g/

16 https://www.itu.int/md/D22-SG02.RGQ-C-0074/

17 For more information on Open RAN security, see for example https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/enhancing-the-security-of-communication-infrastructure_79b78b4d/bb608fe5-en.pdf

## 4. 5G networks and cybersecurity are the focus of recent policy and regulatory initiatives which are at different stages of implementation

### *Example of national policies and regulations to secure 5G networks*

In addition to the standards and practices of vendors and operators, polices and regulations to secure 5G networks can be put forward at the country level. This can take various forms, including vendor assessment, testing, certification, and the establishment of guidelines or requirements. While approaches differ depending on national contexts, these initiatives all aim to mitigate the security risks presented by 5G, including cyber-specific risks. Implementation and compliance regimes should also be considered as part of the overall framework.

The examples below offer a snapshot of different actions and their current status.

- **Brazil**'s holistic approach to 5G cybersecurity focuses on risk management with operators. Under the terms of the 5G spectrum auction and the Cybersecurity Regulation for the Telecommunication Sector[18], 5G operators are required to comply with the regulatory framework, which includes principles, guidelines, and ex ante controls to ensure cybersecurity across the sector. The controls combine cybersecurity governance, mandatory incident notification, information sharing, vulnerability assessment cycles, reporting on critical infrastructure, and other provisions. The Brazilian National Telecommunications Agency (Anatel) has also partnered with academia to conduct studies in this regard.[19]
- The government of the **United Kingdom** developed a security framework for providers of public electronic communications networks or services through the Communications Act 2003 as amended by the Telecommunications (Security) Act 2021 (the TSA). This framework applies to 5G and all other networks: while the UK is transitioning to a 5G and full-fibre future for all networks, many network providers incorporate older technologies within their infrastructure. The TSA sets out new security duties for all public telecoms providers[20] and endows the Secretary of State with new powers to make regulations and issue codes of practice, which have since been developed and informed by public consultation.[21] The Act also includes provisions strengthening Ofcom's regulatory powers to monitor and enforce how providers comply with their new duties.
- The 5G cybersecurity regulations and policies of the **Republic of Korea** are recognized as being among the most stringent globally, reflecting the nation's leading position in the adoption of 5G technology. The national government, through the Ministry of Science and ICT (MSIT) and the Korea Internet & Security Agency (KISA), has implemented a comprehensive framework to safeguard 5G networks. The framework includes stringent cybersecurity requirements for telecom operators to secure network infrastructure, protect user data, and mitigate cybersecurity risks. The regulations emphasize the need for secure supply chains, advanced encryption standards, and the deployment of security-by-design principles in network architecture. Additionally, the Republic of Korea collaborates with international partners and standards organizations to ensure that its 5G security measures align with global best practices.
- The legal and technical framework set up to strengthen 5G cybersecurity in **India** includes:
  - National security directives on the telecom sector, which provides assurance of addressing concerns and vulnerabilities in telecom supply chains and sources;
  - Mandatory testing and certification of telecom equipment, which ensures compliance with essential security requirements for each 5G network function; and
  - Licensing conditions for telecom service providers that include periodic public audits of telecom infrastructure security.

  To support the above, a variety of institutional mechanisms have been put in place: a National Centre for Communication Security (NCCS), mandated to prepare telecom security requirements/standards (Indian Telecom Security Assurance Requirements, ITSARs), with associated security testing and certification labs; the creation of Telecom-CSIRT, a computer security incident response team (CSIRT) for the national telecommunication sector; and a number of citizen-centric measures for fraud management, consumer protection, etc. With regard to security protocols and standards such as 3GPP, India considered specifications proposed by the industry standards for compliance monitoring and further telecom licence conditions that include regular security audits on service providers' networks.
- In the **United Arab Emirates**, securing 5G networks is approached through a multi-pronged strategy that includes rigorous national cyberdrills and training, the establishment of a National Security Operations Center (SOC) for real-time threat visibility and response, and the Cyber Pulse initiative, which raises awareness and trains personnel in key defence strategies. The emphasis is on collaboration and information sharing with international partners, vendors, academia, and other stakeholders to strengthen cybersecurity measures. Additionally, a resilient cybersecurity framework in line with international standards, such as those issued by ISO and NIST, has been set up to ensure compliance across the telecommunications sector. To build consumer and business confidence in 5G security the country has put in place governance policies,

[18] https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740 and https://informacoes.anatel.gov.br/legislacao/resolucoes/2024 (both in Portuguese)
[19] Some of the results are available at https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/estudos-e-pesquisas (in Portuguese)
[20] Except micro entities
[21] https://www.legislation.gov.uk/uksi/2022/933/contents/made and https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

procedures, and laws that promote secure-by-design principles and responsible security practices among vendors. Finally, the country has adopted a people-centric approach to cybersecurity, focusing on training, awareness, and support to empower individuals and organizations in the fight against cyberthreats, thereby cementing a robust defence against potential threats to the 5G network.

- **Zimbabwe** is tackling 5G cybersecurity, focusing on the emerging importance of edge computing and exploring the adoption of open RAN technology for vendor flexibility. While there is no specific 5G security law in Zimbabwe, existing data protection legislation and an in-progress AI governance document underpin the country's approach. Zimbabwe will align its security practices with international standards such as ISO/IEC 27001 and NIST standards, ensuring that new 5G radio interfaces comply with established security protocols. The Postal and Telecommunications Regulatory Authority of Zimbabwe enforces security guidelines and raises industry awareness to maintain the integrity of the national telecom infrastructure.
- **Kenya** adopted its roadmap and strategy for 5G in mobile communications in April 2022. The strategy recognizes that security is an important aspect of 5G network architecture. The evolving nature of connected services and the expected significant increase in the number and types of devices connected lend even greater importance to data privacy, data protection and cybersecurity in Kenya; that includes threat detection, user authentication, and good operational practices. 5G provides better security by design, incorporating enhanced security requirements on the basis of network evolution and adapting what has been learned from earlier technologies. The Communications Authority of Kenya has adopted an approved international standard developed by ITU and 3GPP to ensure interoperability and security of mobile systems. The Authority plans to leverage the expertise of various stakeholders and international best practices in cybersecurity to develop technical codes and implement a standardized minimum security assessment checklist so as to ensure that 5G networks meet the latest technical standards and are in line with global norms in relation to 5G security.
- Following a wide review of the cybersecurity risks to 5G networks, the **European Union** (EU) developed a toolbox of risk mitigating measures[22] with the aim of identifying a common set of measures to mitigate the main 5G cybersecurity risks and help prioritize mitigation measures in EU-level and national-level plans. The Cybersecurity Strategy for the Digital Decade highlights the importance of safeguarding the next generation of broadband mobile network and has a specific appendix on next steps for the cybersecurity of 5G networks.[23] The EU Certification Framework includes the on-going development of a cybersecurity certification scheme for 5G.[24]

[22] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[23] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[24] https://certification.enisa.europa.eu/index_en

### *Implementation and compliance challenges*

Policy development is essential, as is a focus on effective implementation. Reporting mechanisms, compliance with relevant standards, and practical policy and regulatory enforcement measures are necessary to ensure robust 5G network cybersecurity. New frameworks introducing changes for the security of the telecoms networks will necessitate an ongoing compliance journey for telecommunications service providers and therefore close engagement with industry. In the **United Kingdom**, Ofcom uses a supervisory model under its telecoms security regime and engages with the telecoms providers' regulatory and technical teams. The regulator considers that implementation is not only about technical measures – it demands a cultural shift in how telecoms providers think about cybersecurity, requiring them to identify and be accountable for those parts of their networks and services they have outsourced. Engaging at the senior level and getting senior commitment and sponsorship across government, regulators and industry is a prerequisite for success.

In **Malaysia**, the government has approved a new cybersecurity bill which provides that a single agency will manage all critical infrastructures, including telecommunications. The regulator is in the process of developing a set of requirements for operators to report on security compliance. One of the country's operators highlighted that the implementation of the new policy can be challenging as it involves communicating risk and articulating minimum security requirements, which requires time-, cost- and work-intensive concertation, often impinging on shareholder considerations. For operators with shareholders, the structures, policies and regulations in respect of security are sometimes not congruent, which can pose a challenge for security teams. Accordingly there is a need to engage all teams, including C-level officials when considering new security frameworks.

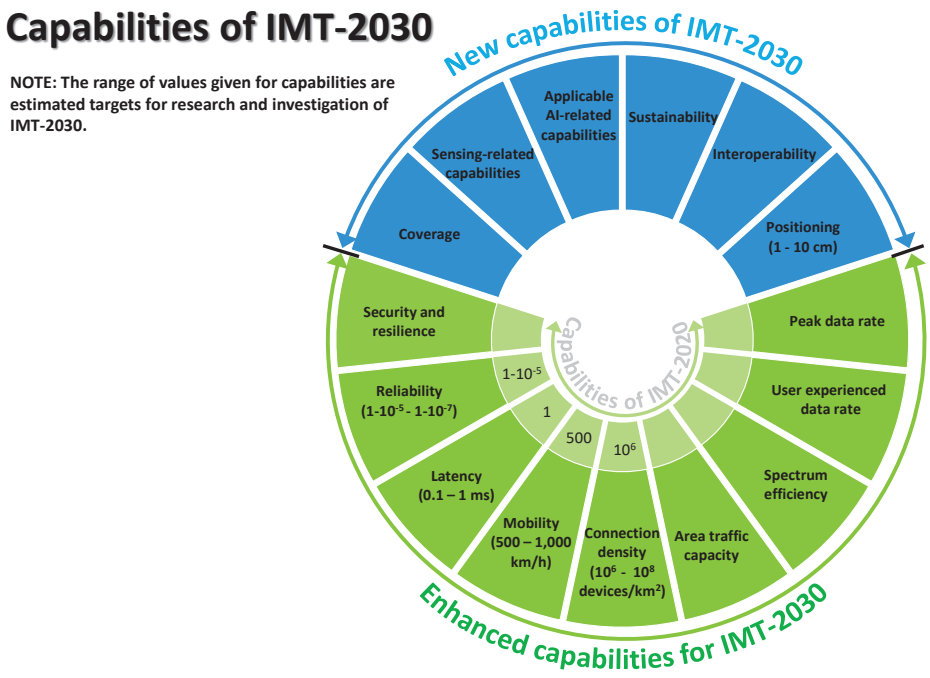
## 5. Investment in educating and training the workforce to handle the complexities of 5G cybersecurity remains a high priority

According to Allied Market Research,[25] the global 5G security market is projected to reach USD 37.8 billion by 2031, with soaring demand for cybersecurity professionals, particularly those with specialized skills for protecting 5G networks. Countries, organizations, and institutions should prioritize workforce training and recruitment to ensure advancement of 5G cybersecurity. The necessary specialized skills are currently difficult to find in the workforce; furthermore, achieving gender balance in hiring is a challenge. If the workforce is not ready, that will slow and complicate the transition to 5G. While countries should prioritize training and education through national programmes, the private sector can also explore training and upskilling programmes, as participation from the wider industry is required to ensure needs are met.

One example of a country that is finding solutions to the workforce challenges is **Türkiye**, with increased investment in educating and training a workforce capable

[25] https://www.alliedmarketresearch.com/5g-security-market-A12820

Figure 1: Capabilities of IMT-2030




Source: ITU-R Recommendation M.2160

of managing the complexities of 5G security. As part of this commitment, a 5G Valley Open Test Site has been established by key institutions, including the Information and Communication Technologies Authority, Middle East Technical University, İhsan Doğramacı Bilkent University, Hacettepe University, and telecommunications operators Türk Telekomünikasyon A.Ş., Turkcell İletişim Hizmetleri A.Ş., and Vodafone Telekomünikasyon A.Ş. This site serves as a vital platform for the research, development, and testing of 5G technologies and beyond, providing opportunities for academic and industry collaboration. The 5G Valley Executive Board, comprising representatives from the aforementioned institutions, ensures the effective implementation of this initiative. By providing a platform where academics, researchers, doctoral students, and start-ups can engage in work related to 5G and beyond, the Open Test Site not only fosters innovation but also contributes to the development of a highly skilled workforce. This initiative is integral to Türkiye's strategy to prioritize and enhance the security of 5G networks through continuous investment in education, training and research.[26]

## 6. Beyond 5G: setting the direction for 6G cybersecurity

Although 5G is still at the planning and deployment stage in many countries and regions, attention in research and development, as well as the standardization processes, is already moving beyond 5G networks. Thus, at the end of 2023 the ITU Radiocommunication Sector (ITU-R) approved the framework and overall objectives of the future development of IMT for 2030 and beyond,[27] commercially known as 6G.

The framework highlights that IMT-2030 is expected to be an important enabler for achieving enhanced security and resiliency. It is expected to be secure by design and to have the ability to continue operating during and quickly recover from a disruptive event, whether natural or man-made. The document also reaffirms that the security and resilience of IMT-2030 systems are fundamental to achieving broader societal and economic goals.

In the context of IMT-2030, security is defined by the framework as the *"preservation of confidentiality, integrity, and availability of information, such as user data and signalling, and protection of networks, devices and systems against cyberattacks such as hacking, distributed denial of service, man in the middle attacks, etc."*. Resilience is defined as the *"capabilities of the networks and systems to continue operating correctly during and after a natural or man-made disturbance, such as the loss of primary source of power, etc."*.

It has become clear that 6G is being envisioned and the start of its standardization processes is being conceived with a robust concern related to security and resilience, in contrast to the early design stages of the 5G technology, including from a standardization point of view. A comparison with the vision for IMT-2020 (commercially known as 5G) approved in 2015[28] compellingly illustrates the shift in thinking with the recognition of the need to properly address cybersecurity and cyber-resilience as an enabling pillar of the digital transformation and digital economy.

[26] https://5gtrforum.org.tr/en

[27] ITU-R Recommendation M.2160, available at https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en

[28] ITU-R Recommendation M.2083, available at https://www.itu.int/rec/R-REC-M.2083-0-201509-I

Follow the work of **ITU-D Study Group 2 Question 3/2 for 2022-2025** Securing information and communication networks: Best practices for developing a culture of cybersecurity

**Question 3/2 website** http://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/questions/Question-3-2.aspx

**Mailing lists:** d22sg3q2@lists.itu.int subscribe here

**ITU-D study groups Web**: www.itu.int/itu-d/sites/studygroups/

Share your feedback on devSG@itu.int Tel: +41 22 730 5999

**ITUPublications**
Published in Switzerland, Geneva, 2024



**International Telecommunication Union**
Place des Nations, CH-1211 Geneva Switzerland