
# 5G security in super-connected operators

5G development has taken place alongside measures to limit the impact to known cyber threats, notably the architectural principle of security-by-design. However, that may no longer be enough. The adoption of new network functions and the establishment of a virtualised and independent core network introduce new potential threats for the industry to manage. MNOs are increasingly connected. Many other industry players are involved. They must work together to ensure the cybersecurity of 5G – and 5G users – worldwide.

**Author:**

Víctor Martínez,
Managing Consultant

**Analysts support:**

Natan Saraf,
Associate

Axon Consulting | October 2022 | axonpartnersgroup.com

# Contents

# Abstract

**Operators are promoting 5G networks as a key part of the supply chain of critical IT applications – and with good reason; 5G has a lot to offer such applications. But this changing role comes with changed security requirements – especially compared with the threat landscapes of previous technology generations – from 1G to 4G – and their networks. The potential threat is new, different and, potentially, greater.**

At the same time many mobile network operators (MNOs) lack experience and knowledge of 5G-specific threats. This can lead them, in many cases, to overlook the need to secure the virtualised 5G environment.

It's true that the advent of 5G has brought with it preventive measures to limit the impact of known threats; the secure-by-design architectural principle is an obvious example. However, the adoption of new network functions and the establishment of an independent core network could introduce new threats. Can the many players now involved in the telecommunications industry work together to manage them?

Network functions were once performed by physical appliances. They are now being 'softwarised', especially at 5G core network level. This increases the impact of failures, due, in part, to a much wider surface area exposure. In short, virtualised environments can be susceptible to a given set of attacks. For this reason, MNOs, together with other industry players, must commit to ensure the cybersecurity of 5G – and 5G users – around the globe.

# Definitions

**Softwarisation** refers to the paradigm where a given functionality runs in software instead of hardware. A migration from hardware-based to software-based solutions. This approach guarantees high degree of flexibility and reconfigurability as functionalities can be enhanced by updating the software.

**Virtualisation** enhances the software/hardware splitting of the softwarisation approach by creating abstract (virtual) instances of hardware platforms, operating systems, storage devices, and computer network resources. This means that, with virtualisation, software runs in commercial off-the-shelf equipment by exploiting a virtual machine (VM) instead of a dedicated hardware.

**Network function virtualisation (NFV)** is a network architecture concept that provides the enabling technology for placing the network functions in the form of virtual machines and/or containers in commoditised infrastructure (i.e. servers) on the basis of performance needs, abstracting these from the hardware on which they run. With NFV, network node functions (such as firewall, switches, routers, etc.) are virtualised and thus totally decoupled from the underlying hardware running such functions.

**Software defined networking (SDN)** is a network architecture approach seen as the main realisation of the softwarisation concept. It enables the network to be intelligently and centrally controlled, or 'programmed,' using software applications. SDN introduces the possibility of decoupling network control from forwarding functions and thus allowing flexibility and reconfigurability of the physical network.

**Micro-services based architecture** is used for building a distributed application by arranging it as a collection of independent, loosely coupled, individually deployable services that handle discrete tasks. Each microservice communicates with other services through simple interfaces to solve business problems.

**Containerisation** is an alternative or companion to virtualisation. Containers are a lightweight, efficient and standard way for applications to move and run independently between environments. Everything needed to run the application is packaged inside the container object, including the code, dependencies, libraries, and others.

# 1. Introduction

The fifth generation of cellular networks (5G) has a lot to offer: value-added services with advanced performance such as low-latency communications, high reliability, and high data rates, to name only a few. It also promises to supply the vast capacity required to support an increasing number of connected devices across diverse sectors of the economy. It's no exaggeration to say that 5G is ushering in a new era. It will not only offer many more technical capabilities; it will also revolutionise both commerce and people's lives.

5G is also a different network technology from anything that has come before. For example, it introduces a new core based on a virtualised, cloud-based architecture. This in turn enables highly specialised functions and security for different network applications.

This 5G virtualised revolution brings with it security that is much more advanced than previous generations. However, inevitably, it also brings security challenges: softwarisation is one of the most significant. The softwarisation of the network expands the attack surface for cyberthreats. Managing this has meant introducing new security functions and implementing architectural principles of security-by-design from the early stages of the design and deployment of 5G networks.

This approach means 5G is much more secure from the design point of view. However, features inherent to 5G micro-services architecture – such as network function virtualisation (NFV), software defined networking (SDN), or containerisation – make security analyses more complex. This is because they involve more industry players – both traditional ones and new third-party players.

**This 5G virtualised revolution brings with it security that is much more advanced than previous generations. However, inevitably, it also brings security challenges.**

Of course, 5G is also the fastest generation in terms of downloading and uploading. This could benefit cyber attackers. Reaction times to attacks need to be faster than ever.

Despite this it is sometimes the case that MNOs overlook the necessity for secure 5G environments, either because they lack experience or because their experience is only of known 5G-specific threats. But MNOs are both ubiquitous and the entry point for this technology to billions of users and devices. They must therefore work with other industry players and have in place appropriate cybersecurity measures while building their 5G networks in order to be able to deal with numerous potential types of cyber-attacks.

This paper explores the main security advantages – and challenges – of 5G, and offers a set of best practices that MNOs can follow.

# 2. Security advantages of 5G to older generations

The first generation of cellular networks mainly involved person-to-person voice calls. Written texts joined voice calls in the second generation (2G). The third generation and GPRS revolutionised the connectivity landscape by connecting people to the Internet. The fourth generation (4G) generalised the usage of the internet protocol (IP) for all services (voice, data, messages, video). It also provided higher bandwidths, internet-connected apps and a vastly improved user experience. The fifth generation – 5G –links people on a massive scale with connected devices in real time, increasing bandwidth and lowering latency. It's a vast improvement in the end user experience.

But the introduction of new generations has not completely replaced the previous ones; the evolution and expansion of networks over time has brought with it the interconnection and reuse of elements from previous generations alongside new ones. This has meant greater complexity, increased vulnerabilities and a larger cyber-attack surface. Put another way, the security of a chain of networks is defined by its weakest links.

**The evolution and expansion of networks has brought with it the interconnection and reuse of elements from previous generations. This has meant greater complexity, increased vulnerabilities and a larger cyber-attack surface.**

Of course, ensuring network security is a high priority for operators and it hasn't got any easier with new attack vectors and threat actors. For this reason, 5G network components were initially built on the basis of security-by-design principles. The goal was to learn from the past and mitigate in this new generation the vulnerabilities and risks witnessed in former ones. This means traditional security considerations aimed at protecting networks and subscribers are less of an issue for 5G than for previous generations.

**Ensuring network security is a high priority for operators and it hasn't got any easier with new attack vectors and threat actors.**

This, however, is not the whole story.

## 2.1. What does security mean for mobile telecommunication networks?

The first generation of mobile networks was pioneering. However, that also meant it was vulnerable to cyber-attacks that could compromise operators' and users' security. As MNOs worked to ensure greater security in the following generations, they were influenced by security concepts, not just derived from mobile networks but also from computer networks. In particular, operators were inspired by the so-called security triad to ensure **confidentiality, integrity and availability** (CIA) – an approach centred on data and information systems. MNOs' security architectures have been informed by these three key attributes ever since.


Exhibit 2.1: The security triad [Source: Axon Consulting]

**Operators were inspired by the so-called security triad to ensure confidentiality, integrity and availability, an approach centred on data and information systems.**

All the elements of the security triad aim to protect individuals or entities that possess or transmit data – in any form. Confidentiality ensures that data (normally subscriber data) is accessed only by authorised individuals or entities. Integrity prevents the modification of that information by unauthorised users. Availability makes sure that data is available on demand to authorised parties.

Data is a principal and highly valued asset that is vulnerable to attacks while it is processed, stored or transmitted within networks. Not surprisingly therefore, mobile network architectures are now more than ever rooted in reliability and security approaches based on the CIA triad to ensure a seamless, end-to-end protection of the entire network.

## 2.2. Evolution of security measures in mobile telecommunication networks

**The concept of telecoms network security has evolved with each technology generation.**

Modest security measures were adopted in the early days of MNOs. However, that quickly changed and cybersecurity was soon seen as the major challenge for the world of information and communication technology. Each new mobile communications generation was built upon stronger precautions than the previous one in an attempt to block emerging threats and take on the ingenuity of hackers with new and similarly ingenious responses. The concept of telecoms network security has evolved with each technology generation, demonstrating the increasing ability of operators and network developers to continuously confront the threat landscape. At the same time this is an unavoidable requirement: the security measures employed to ensure secure processing of analogue signals in 1G differ greatly from the measures needed in today's vast 4G/5G cloud infrastructure.

| Mobile network generation | New security measures |
|---|---|
| 2G | ■ Authentication of a user<br>■ Ciphering of data and signalling<br>■ Confidentiality of user identity |
| 3G | ■ Network access and domain security<br>■ User domain and application security<br>■ Visibility and configurability of security |
| 4G | ■ Data encryption<br>■ LTE authentication<br>■ Secure signalling |
| 5G | ■ Secure-by-design<br>■ IP and cloud security standardised<br>■ Zero trust approach for all 5G cloud infrastructure |

Exhibit 2.2: New security measures adopted in each new mobile network generation [Source: Axon Consulting]

As we have noted then, every new generation came with its own new set of security measures. However, 5G was truly innovative, embracing new approaches to mitigate past problems from minute one. In fact thanks to the **secure-by-design** concept, security is the number-one priority for 5G. In fact 5G's inbuilt security advantages and ground-breaking characteristics are reshaping cybersecurity solutions in the ICT world.

**The security measures employed to ensure secure processing of analogue signals in 1G differ greatly from the measures needed in today's vast 4G/5G cloud infrastructure.**

## 2.3. The technical advantages of 5G cybersecurity

Thus, while every generation from 2G to 4G developed new defence mechanisms for various threats, 5G developers created a much more secure network from the design point of view – one that included built-in defence features that older generations and protocols lacked. Previous generations reacted to threats; 5G has been proactively designed to keep away threats. It includes updated features from its ancestor generations together with innovative new ways of dealing with cybercrime.

A clear example of this evolution is **data encryption**. Data encryption was already a part of 4G security measures designed to provide anti-tracking and spoofing features and to prevent the manipulation of individual device connections by unauthorised parties.

But 5G is a cloud-based system; more data has to be encrypted. For instance, subscriber identifiers were subject to attacks in previous generations due to the transmission in the air interface. Enhanced subscriber identity protection is part of the 5G package; 5G encrypts the identity before it is transmitted.

**Mutual authentication** was also introduced with 4G, enabling two or more devices to be connected. The risk here was that an attack on one device could affect all mutually authenticated devices. With 5G, additional authentication considerations were part of the design phase. Cyber attackers who gain access to a given device will no longer have easy access to other linked authenticated devices.

**Network segmentation** was perhaps one of the key advances in the transition from 4G to 5G, helping to isolate environments and enable operators to carry out a separation of their systems in various ultra-secure networks. These sub-networks are managed separately; customised protection for each of them ensures a more secure overarching network.

Besides updated features from past generations, 5G is, by default, built on security standards. This makes its network architecture truly one of a kind.

**5G developers created a much securer network from the design point of view – one that included ready-built-in defence features that older generations and protocols lacked.**

To complement the robustness of 5G security standards, any operator willing to deploy a secure-by-design network needs to adopt the following security principles:

1. **Least privileges** – individuals should only have access to what they need to properly carry out their duties – and nothing beyond that.

2. **Need-to-Know** – sharing should involve only the required information and level of knowledge between individuals (in a specific company department, say) for carrying out their tasks – and nothing beyond that.

3. **Segregation of duties** – duties should be separated in order to avoid giving too much power to a single individual. Tasks and privileges for a specific security process should be shared out among multiple people.

4. **Avoid security by obscurity** – if an application is secure only when is hidden or when the secrecy or confidentiality of its internal architecture exists, then it is not secure enough. Other measures must be used.

5. **Network segmentation** – networks should be divided into multiple segments to improve security and spread the risk when a potential breach occurs.

6. **Zero trust** – every person and entity accessing the network systems (that is, the cloud) is by default untrusted and must be checked.

7. **Secure defaults** – the default configuration of network elements should reflect a restrictive and conservative enforcement – for eample denying access unless explicitly authorised.

8. **Attack surface reduction** – rules should be employed to identify and reduce the area of an organisation's attack surface that is susceptible to hacking.

It seems clear that at the heart of 5G are reliable procedures to ensure the confidentiality, integrity and availability of the entire network. That is, 5G really does offer a unique security experience.

However, the technology is still used in limited geographies with limited exposure to, and experience of, real life 5G-specific threats. Various new security challenges are already being discussed. Additional, so far unknown, risks may arise as the adoption of 5G technology spreads across the world.

# 3. Security challenges of 5G

The definition of security in mobile telecommunication networks has evolved with the arrival of emerging technologies such as 5G. New threats are being added to the definition of telecommunications cybersecurity. In fact although 5G is an emerging technology, security issues are still targeting the CIA triad. For example, data interception in the 5G network may affect confidentiality; destruction of digital infrastructure through 5G networks could be a threat to their integrity; and a 5G network disruption could potentially harm local or global network availability.

There's another issue. 5G networks will in all likelihood end up being an important part of the supply chain for many critical IT applications. This makes threats to 5G networks very different from threats to existing networks simply because of the nature and intensity of their potential effect. Yes, confidentiality and privacy requirements could be impacted. But so too could the integrity and availability of 5G networks, resulting in major national security concerns and a major security challenge. And if 5G networks play a greater role in economic and societal how much worse could the consequences of disruptions be?

**5G networks will in all likelihood end up being an important part of the supply chain for many critical IT applications. This makes threats to 5G networks very different from threats to existing networks.**

Again, we must remember that the advent of 5G has brought with it preventive measures to limit the impact to known threats, especially with the secure-by-design architectural principle. However, the adoption of new network functions and the establishment of an independent core network introduce potential new threats.

The full adoption of IP protocol and technologies used in IT environments and computer networks (virtualisation and the cloud, to name only two) increases the exposed surface. And don't forget, hackers were already familiar with these technologies and looking for vulnerabilities within the same protocols and operating systems. In parallel, the concept of open source, widely used by companies commercialising 5G products, is a double-edged sword. On the one hand, the code is exposed; anyone with sufficient knowledge and motivation can find a bug to exploit. On the other, there are more 'honourable' hackers keen to find and expose such problems to focus on gaps in security.

**The adoption of new network functions and the establishment of an independent core network introduce potential new threats.**

One of the most important innovations in the 5G architecture is the complete virtualisation of its core network. There has been a softwarisation of network functions that were once performed by physical appliances. This high level of virtualisation increases the impact of failures because of a much bigger exposed surface.

## 3.1. The 5G core

The core can be a highly vulenerable layer of any telecommunications network for the simple reason that the most sensitive data is transmitted through its components. The 5G core, for example, involves a service-based architecture whereby key functionalities are delivered thanks to a set of interconnected network functions, each of which has authorisation to access any other function's services. This close interrelation means 5G core network functions become critical assets. Anything adversely affecting the 5G core network could also compromise the confidentiality, integrity and availability of the entire array of network services. By contrast if other components outside the core are compromised, this may only affect a standalone function or area.

To enable scale, throughput, latency, and reliability, 5G architecture was designed so that connectivity and data services coulds be supported. To ensure this, 5G architecture natively adopts network function virtualisation (NFV) and software defined networking (SDN) together with container technologies in order to implement a micro-services architecture that streamlines network and service deployment, operations and management. This micro-services-based architecture meets multiple functional and performance requirements built upon new use cases in a cost-efficient way.

**5G architecture natively adopts Network Function Virtualisation (NFV) and Software Defined Networking (SDN) together with container technologies in order to implement a micro-services architecture.**

### 3.1.1.
## Transition to a virtualised core: NFV and SDN

NFV and SDN both use abstraction. NFV, for example, provides an enabling technology that allows the placing of network functions in the form of virtual machines and/or containers in commoditised infrastructure (i.e. servers) on the basis of performance needs, abstracting these from the hardware on which they run. Both are types of virtualisations that allow network functions or components to be deployed, managed and operated in a more agile, massive (and cost-effective) way over a more uniform and versatile infrastructure composed of servers and their corresponding operating systems.

SDN, by contrast, brings simplified management together with innovation to separate network control functions from network forwarding functions. This is a major shift from traditional network architecture. Functions are longer built upon specialised hardware and software; functionality and differentiation solely take place in software.

NFV and SDN are fundamental to the networks of the future. That's because they open the door to flexible networks and rapid creation of services. NFV and SDN complement each other by improving network elasticity, simplifying network control and management, and overcoming the obstacle of vendor-specific or proprietary solutions.

From a security perspective, virtual and cloud-native network functions may also bring certain benefits by allowing for facilitated updating and patching of vulnerabilities. However, at the same time, such increased reliance on software introduces additional security challenges and complexities.

## 3.1.2 Micro-services and containerisation

Another key element of the cloud-native 5G core involves the link between micro-services and containerisation. A micro-services architecture is used for building a distributed application by arranging it as a collection of independent, loosely coupled, individually deployable services. In a micro-services architecture, services are fine-grained and containers are utilised as a lightweight, efficient and standard way for applications to move between environments and run independently. The idea is that teams can bring their services to life independent of others , making this a resilient and scalable architecture.

If an architecture is to be virtualised, one can leverage machine virtualisation, that is, virtual servers on servers. Alternatively one can leverage containers, which are based on operating system virtualisation, allowing applications running in a container to see their own operating system, independent of the rest of the applications in other containers.

Containers are more efficient in their use of computing resources, but the high performance required by data plane applications is more easily achieved today with virtual machines (VMs).

That said, many people believe that containers are the future. However, VMs and containers will coexist for a long time. VMs facilitate the use of products and applications that have not been completely re-architected, while containerisation requires a complete re-architecture based on micro-services, often referred to as cloud-native. In any case, it is possible to combine these technologies and run containers on top of VMs and vice versa. Thus one should look at these technologies as tools with different objectives and not necessarily as antagonistic.

## 3.2
## 5G core security challenges

The virtualised, cloud-native 5G architecture we have described enables highly specialised functions and security for different network applications. However, the higher degree of softwarisation significantly increases the exposure to third-party suppliers (meaning a much wider attack surface). The new and complex threats faced increase the importance of robust patch management procedures and frequent updates. Put another way, if not managed properly, 5G core's new intrinsic features are expected to increase the overall attack surface and the number of potential entry points for attackers; they will also increase the chances of malicious impersonation of network parts and functions.

**5G core new intrinsic features are expected to increase the overall attack surface and the number of potential entry points for attackers.**

It's true that network operators have little experience of this. It's also true that the number of 5G-specific network attacks is so far modest. Nevertheless, we can anticipate a number of security challenges likely to be faced by this innovative technology. For example, thre's evidence that virtualised environments can be susceptible to forwarding device attacks, control plane threats, API vulnerabilities, or counterfeit traffic flows, among others.

Here are the most common types of these challenges, principally related to nefarious activity or abuse of NFV and SDN assets:

- **Memory scraping** – this threat arises when an attacker scans the physical memory of a software component in order to extract sensitive information that it is not authorised to have. While memory scraping can affect components of any layer of the network, this type of threat primarily involves attacks on SDN application servers to exploit private data.
- **Denial-of-service** – DoS is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks include flooding, amplification, signalling storm and saturation, compromising network component availability. This event may also come in distributed DoS (DDoS) attack form, where a vast number of sources may orchestrate multiple attack vectors.
- **Eavesdropping on subscriber data** – this is a threat in which the perpetrator seeks to tamper with the application and communication layers in various 5G network elements. It includes eavesdropping on subscriber data, confidential information, or subscriber location, among others.

**Virtualised environments are found to be susceptible to forwarding device attacks, control plane threats, API vulnerabilities, or counterfeit traffic flows.**

- **Traffic sniffing** – this is a popular way of capturing and analysing network communication information. Sniffing can happen anywhere where there is constant traffic, taking advantage, for instance, of unencrypted communications to intercept traffic.

- **Manipulation of network configuration/data forging** – This threat involves compromising a core network element by forging configuration data to launch other attacks (such as DoS), specifically affecting configuration and/or control plane data.

- **Software exploitation** – this threat enables a malicious actor to take advantage of unknown or unpatched software flaws to perform an attack. It also includes the exploitation of other known vulnerabilities related to previous generations of mobile telecommunications and older signalling protocols such as SS7 (Signalling System 7) and Diameter.

- **Remote access exploitation** – in this case a malicious actor has remote access to critical network components and takes control of a VM to perform other types of attacks. With access to a VM in the network, a malicious actor can engage in other activities such as tampering with configuration data and distribution of malware.

- **Network virtualisation bypassing** – bad network slicing implementation, or improper configuration or isolation, can cause loss of data confidentiality and privacy. Ensuring traffic isolation by installing legitimate flow rules preventing slice trespassing is key to avoiding this.

- **Mixed virtual and legacy (physical) deployments** – in the current form of virtualisation deployment, operators are incorporating both NFV and containerised components into networks with legacy devices. The security challenges raised by operators managing hybrid (part physical, part virtualised) network environments should be considered when deploying 5G telco management and orchestration architecture.

# 4. Ubiquitous operators and their role in 5G cybersecurity

Each iteration of mobile network generations has brought new features to the ICT sphere, some of these focused on cybersecurity. The introduction of 5G represents a major transition for MNOs compared to previous technological evolutions since new functions and processes inherent to 5G inevitably drive current networks to adopt innovative designs. MNOs are the entry point for this technology to billions of users and devices around the globe. As they become ever more connected, MNOs must work with other industry players and follow appropriate cybersecurity measures to ensure the safety of the 5G environment against numerous potential types of cyber-attacks.

**Increasingly connected MNOs must follow adequate cybersecurity measures to maintain 5G environment safety against numerous potential types of cyber-attacks.**

## 4.1. Interconnected network operators

MNOs have an essential decision-making role in the 5G cybersecurity environment; they are, after all, the main stakeholders. To keep network operations secure, an automated and systematic security mechanism is key to an MNO's approach to 5G cybersecurity. As 5G networks involve a wider range of already established stakeholders (such as equipment manufacturers) plus the incorporation of new ones (for example third-party service providers such as virtualisation platform suppliers), shared overall security responsibility is essential. MNOs are not alone. They must work with other actors that hold specific and unique roles in the ICT world – from major industry players to the newest entrants in the market.

Well-known telecom equipment manufacturers such as Ericsson, Cisco, Huawei, or Nokia provide software and hardware needed for operating networks with the latest technologies. However, NFV and SDN have lowered the barriers to the development of software-based network functions. This has allowed new players such as Mavenir, Affirmed Networks, Altiostar and many others to enter the market. All of them, new or established, participate in the standardisation process of 5G cybersecurity alignments through the different components offered in

the market. Some MNOs tend to work with a single equipment supplier. Others prefer multiple vendors. Either option is valid. However, care must be taken to ensure that diverse operations are compatible and to guarantee secure, flawless system integration.

On the other hand, MNOs also interact with third-party suppliers who provide multiple services maintaining and managing data or (virtualised) networks. With Open RAN technology, MNOs tend to diversify the third parties that they rely on, and new names appear, such as virtualised infrastructure service providers or data centre service providers. The major risk here is the poor familiarity of new third-party players with security approaches. Some may prioritise innovation to the detriment of network security.

## 4.2. MNOs best practices to ensure 5G cybersecurity

**MNOs *must* lead the cybersecurity charge by example, following the best industry approaches towards 5G network security.**

With this emerging number of players orbiting around operators, the attack surface increases, offering more space for cyber criminals. MNOs must lead the cybersecurity charge by example, following the best industry approaches towards 5G network security.

Here we outline a set of best practices for MNOs to limit and manage potential entry points for attackers – right from the start.

1. **Appropriate network design and architecture.** This is critical. Ensuring a correct network design and adhering to best architectural principles can reduce the vulnerability of the 5G core network (and the network as a whole). This approach includes, among other factors, paying attention to the firewalling of the different core networks and components, the adoption of effective emergency and continuity mechanisms, and having a thorough network systems configuration (for example in virtualisation, in administration or in access rights). the overall aim is to significantly reduce exposure to negative consequences such as lack of isolation of low-trust systems or unnecessarily large security breaches.

2. **Adequate security and operational maintenance procedures, such as periodic software updates and patch management.** This becomes much more acute for MNOs when dealing with 5G networks, given the higher reliance on software systems (for example the cloud) and the much higher frequency of maintenance and system patching required to ensure security and functionality and to minimise the network's exposure to unnecessary risks.

3. **Implementation of suitable (cyber)security controls, monitoring practices and risk management.** Following industry standards and/or internally created cybersecurity controls makes it easier to prevent or reduce security risks to physical and virtual assets that can be caused by error, accident, or malicious action. Likewise, MNOs must incorporate state-of-the-art network management and monitoring systems; these are fundamental to a quick and accurate response to potential threat situations or vulnerability disclosures. Additionally, effective risk management and mitigation should be based on robust and regular risk assessments.

4. **Compliance with 3GPP/GSMA standards and correct implementation.** 5G standards aim to be more secure than those from previous technology generations. Thus, although standards surrounding 5G continue to be researched and developed, MNOs should comply with top-tier standardisation bodies. This will help them to establish an adequate baseline of security measures that guarantee 5G network cyber-resiliency from the ground up.

5. **Well-defined policies for local/remote access to network components and subscriber data protection.** Locally or remotely accessing the myriad network components, devices and virtual appliances characteristic of 5G networks should be governed by an overarching access control policy that MNOs should ensure is well defined. This becomes even more critical in virtualised environments where maintenance is carried out by third-party suppliers and subscriber data can be accessed. Subscriber data protection policies are fundamental; they should be defined alongside other 5G security policies.

6. **A specialised and trained workforce to maintain, monitor and secure 5G networks.** A company will be secure if the employees are aware and trained to manage the fast-evolving threat landscape and the complexity of 5G networks. MNOs should ensure that they have IT security professionals at hand with specialised know-how – based on work in the field – to manage and operate any 5G-related aspect of their network.

Many of the measures suggested above are not specific to 5G networks. However, 5G technology is much more complex than any that has preceded it. In addition whole economies and societies will rely on 5G to a greater extent than any earlier mobile technology. It is therefore more important than ever that these measures are implemented in the 5G era.

# About
# **Axon Consulting**

Axon is an international firm founded in 2006 that provides investment and advisory services to a broad client base in the technology and innovation space in more than 70 countries across the world.

Axon's cybersecurity practice is central to its business and an increasingly important service area for clients. Its work in this field includes strategy, policy/regulation, and research at business and governmental level. Axon works closely with national representatives to help them understand their cybersecurity needs and to define actionable recommendations aimed at improving their cybersecurity ecosystems.

**Tel:** +34 913 102 894
**Email:** marketing@axonpartnersgroup.com



**Madrid (HQ)**
Calle Sagasta 18,
3rd Floor,
28004, Madrid

**Brussels**
91, Avenue du Roi,
1190, Brussels

**Istanbul**
Buyukdere Cad.
No. 255 Nurol Plaza,
B0434450 Maslak,
Istanbul

**Bogota**
Calle 100 #13-95,
Torre Empresarial FD,
100 Piso 6,
Bogota

**Riyadh**
3141 Anas ibn,
Malik Road, Building B,
2nd Floor,
Al Malqa, Riyadh

**AxonPG**

**axon-partners-group**