5G Security Report

China Academy of Information and Communications Technology（CAICT）

IMT-2020(5G) Promotion Group

Feb. 2020

Contents

Foreword

Around the world, the scientific and technological revolution, as well as industry transformations, are in full swing. And as next-generation information and communication technologies (ICTs) continue to evolve and the Internet of Everything (IoE) takes shape, 5Gtakes center stage as a critical information infrastructure that enables such developments and drives the digital transformation of both our economy and society. Accelerating the development of 5G and deepening its converged application in various aspects of our economy and society will have multifaceted and profound impacts on the politics, economy, culture, society, and many other areas. It will reconstruct the global innovation landscape and reshape the global economic structure. Major countries in the world regard 5G as a top priority in their economic development and technological innovation, and consider it to be a major strategic direction for advancing their competitiveness. According to statistics from the Global mobile Suppliers Association (GSA), as of October 2019, 348 telecom operators in 119 countries or regions around the world had invested in 5G, of which 61 had already launched commercial 5G services.

Every coin has two sides. While 5G benefits society and the people, it also poses network security risks. The President of the People's Republic of China (PRC) pointed out at the Second World Internet Conference that maintaining cybersecurity is the joint responsibility of the entire international community. With this in mind, the international community should strengthen dialogue and cooperation on the basis of mutual respect and trust, with the aim of jointly building a peaceful, secure, open, and cooperative cyberspace. 5G security is not just an issue for a select few countries, it is something every country must face. This is why we must embrace the concept of open and cooperative cybersecurity. And when addressing 5G security risks, it is imperative that we are objective and strive to deepen cooperation, enhance mutual trust, and jointly improve 5G security protection.

Against this backdrop, China Academy of Information and Communications Technology and IMT-2020(5G) Promotion Group — a professional research institute in China's 5G field — jointly prepared this report based on previous research and recent investigations. The purpose of the report is to address security risks is terms of key technologies, typical application scenarios, and industrial ecology, as well as to detail the corresponding security concepts and protective measures, with the aim of strengthening mutual trust and cooperation between all parties and promoting the development and security of 5G.

I. The Significance of 5G Development

1. 5G is the latest achievement of global information technologies. Having evolved through multiple generations, from 1G to 4G, mobile communication networks have now entered a critical stage — 5G. What sets 5G apart from previous generations is the shift from purely people-to-people communication to that of people-to-things and things-to-things. This change presents all-new opportunities for ubiquitous connectivity of all things, deep human-machine interactions, and intelligence-led transformation. As 5G develops, it becomes an ecosystem in its own right, bringing countries and regions together and allowing their respective technologies, products, and services to flow more efficiently. In this way, all countries — not only a select few — are able to benefit from 5G. The global industry and academia worked together to release the first version of the 5G standard (R15) in June 2018. This important milestone laid a solid foundation for the formation of a globally aligned 5G industry ecosystem. Such a result was no mean feat.

2. 5G can drive economic growth. The Fourth Industrial Revolution —characterized by digitalization, networking, and intelligence — is now well under way, presenting new drivers for the growth of the world economy. A study by the World Bank concluded that a 10 percentages point increase in fixed broadband penetration would increase GDP growth by 1.21% in developed economies and 1.38% in developing ones. And when it comes to mobile communications, 5G is going to be the critical infrastructure for IoE. It is already being applied in fields as varied as mobile Internet, industrial Internet, Internet of Vehicles (IoV), and Internet of Things (IoT). 5G can support digital transformation in more scenarios, to a deeper level, and with higher standards, as well as unleashing economic benefits driven by ICT. According to IHS Markit[1], 5G will generate a global economic output worth $13.2 trillion and create 22.3 million jobs by 2035.

[1] IHS Markit: "How 5G technology contribute to the global economy", The 5G Economy, Nov. 2019

3. 5G will create new models of smart society. The integration of 5G with other emerging technologies such as cloud computing, big data, and artificial intelligence (AI) will help form a data-driven and scientific decision-making mechanism, as well as promote innovation in government management and social governance models. By leveraging features of 5G, such as wide coverage, large capacity, high speed, and low latency, we can promote the deep integration of 5G-centric intelligent infrastructure with urban governance. In this way, we can improve the urban living environment through applications such as traffic management and environmental monitoring, promote smart city operations that offer intelligent perception, precise management, and convenient services, and create healthy, comfortable, and environment-friendly urban living spaces for the people.

4. 5G will expand the meaning of people's livelihood and well-being. 5G is going to become a vital means by which people's livelihood and well-being are improved. It is able to fully support personalized and intelligent services, improve ways of living, and enhance people's quality of life. 5G offers more varied information and communication services for the public, creates more effective supplies in line with consumption upgrades, reduces the cost of information consumption for society as a whole, and effectively bridges the urban-rural digital divide. Regarding public services, 5G can improve efficiency, achieve precise matching and effective docking between supply and demand, and provide new models such as distance education and smart health. 5G also promotes the sharing of high-quality resources and enhances people's sense of gain and well-being.

II. Overview of 5G Network

In 2015, the International Telecommunication Union (ITU) released the "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond", which identified three new application scenarios: enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (uRLLC), and massive machine-type communications (mMTC), as well as eight key performance indicators (KPIs) such as peak rate and traffic density. Regarding these KPIs, 5G performs very highly, reaching 10 times the peak rate of 4G, shortening transmission latency to milliseconds, and handling a million concurrent connections per square kilometer.

1. 5G network architecture and key technologies

5G has largely inherited the same network architecture used in 4G, including the access network, core network, and applications on the upper layer (as shown in the figure below). However, to meet the diverse business needs of 5G mobile Internet and mobile IoT, 5G has also evolved significantly by introducing new innovative technologies to both the core network and the access network.

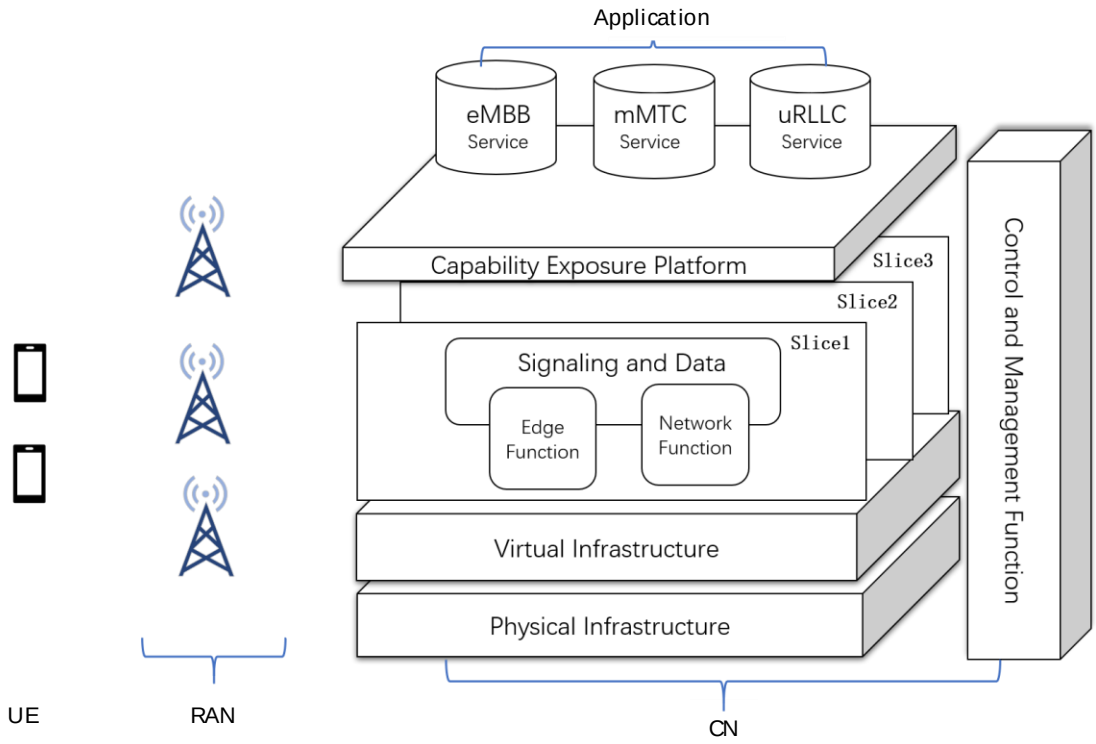

Figure: 5G Network Architecture

The key technologies used in 5G include:

- **Service-Based Architecture (SBA).** In 5G SBA, network functionality of a network function entity is provided as a service towards external request (from other network functions). Different network functions and services communicate with each other through standard APIs(Application Programming Interfaces) to support on-demand configuration and restructuring of network functions, thereby improving the flexibility and openness of the core network. 5G SBA is an important means for rapidly meeting the needs of vertical industries in the 5G era.

- **Network Function Virtualization (NFV)**. 5G uses virtualization technology to decouple software and hardware of dedicated network elements to form a unified virtual infrastructure based on which network functions are constructed. Benefits of this include centralized control, dynamic configuration, efficient provisioning, and intelligent deployment of resources, which serve to shorten the business innovation cycle for network operations.

- **Network Slicing**. Network slicing can be leveraged to separate one physical network into multiple logical networks, each with different network functions and features combination. In this way, multiple business scenarios can be supported at the same time. The advantage of this is highly improved network resource utilization and isolation of network resources between different business scenarios.

- **Edge Computing**. Multi-access edge computing (MEC) provides computing and data processing capabilities at the edge of the network, close to users. It improves the network's data processing efficiency and provides the low latency, high traffic handling, and security required by vertical industries.

- **Network Capability Exposure(NCE).** 5G supports the exposure of network capabilities to third-party applications through the capability exposure APIs, thereby allowing third parties to design customized network services based on their own needs.

- **Key Technologies of the Access Network.** 5G uses a flexible system design for the access network, allowing it to support multiple services and scenarios. In addition, its adoption of new channel coding schemes and massive MIMO technologies help to realize high data-rate transmission and better coverage.

In addition, the 3rd Generation Partnership Project (3GPP) has clearly defined the interfaces between the access network and the core network, which have been shown to have different functions and clear boundaries. Industry experts[2] have expressed their views that, despite a few core network functions being

[2] The views expressed by Professor Alf Zugenmaier, Vice Chair of 3GPP SA and the expert from Munich University of Applied Sciences at a public hearing on "Britain's telecommunication infrastructure" of the Science and Technology Committee of Britain's House of Commons in June 2019. https://www.parliamentlive.tv/Event/Index/65f2ce0c-2994-46b2-bd9b-3b10dc38ca6f

deployed at the edge in 5G, the functional boundary between the access network and the core network remains unchanged. And to further improve security, a security gateway can be deployed between the core network (including edge computing part) and the access network. Taking all of this into consideration, it is also an effective way for operators to diversify their supplier selection of the access and core network products to improve network resilience.

2. 5G security framework

5G security includes both the end to end communication security within the network (e.g. between device and gateway), and the security of applications running over the network. The reliability and security of the mobile communication network have been considered specifically since the beginning. After decades of global joint efforts of the mobile industry, the security architecture of mobile communication networks has become very stable and well designed.

5G has adopted the same layered and domain-based security architecture that is used also in 4G. It is specified in the 3GPP 5G security standard — “Security architecture and procedures for 5G System”[3] — that 5G uses exactly the same security stratums as 4G — transport stratum, home stratum/serving stratum and application stratum — with each stratum isolated from each other. In terms of security domains, the 5G security framework has added a new 'SBA domain security' to the overall security domains based on 4G — network access security, network domain security, user domain security, application domain security, visibility and configurability of security.

5G provides stronger security capabilities than 4G, including:

- **SBA domain security**. In response to the security risks brought about by the new 5G SBA, 5G uses comprehensive registration, detection, and authorization security mechanisms and protocols to ensure SBA domain security.

- **Enhanced protection of user privacy**. 5G networks use encryption schemes to transmit the user identity. This prevents attackers from

3 3GPP TS 33.501: "Security architecture and procedures for 5G System"

exploiting the plain-text transmission of user identity over the air interface for illegally tracking the user's location and obtaining information.

- **Enhanced integrity protection**. 5G networks leverage encrypted protection of user plane data over the radio interface to further ensure the integrity of user plane data and prevent such data from being tampered with.

- **Enhanced inter-operator roaming security**. 5G networks can provide end-to-end protection for the inter-operator signaling between network operators and prevent man-in-the-middle attacks that are used to obtain sensitive inter-operator data.

- **Unified authentication framework**. On 4G networks, different access technologies are used, each with different authentication methods and processes. This makes it difficult to ensure the continuity of the authentication process between heterogeneous networks. 5G overcomes this issue by adopting a unified authentication framework, which integrates multiple authentication methods of different access types.

In summary, 5G provides standardized solutions and stronger security protection mechanisms to meet the enhanced security needs of SBA, privacy protection, authentication, and authorization.

III. 5G Security Concepts

5G is a key information infrastructure and an important cornerstone of digital transformation. As such, it not only presents a new landscape for IoE, but also poses new security challenges and risks that all countries must face. This calls for all parties to work together towards the common goal of network security featuring openness and cooperation, and to look at and respond to 5G security risks in a comprehensive and objective manner.

1. Looking at 5G security from a development perspective. 5G is the latest achievement in the development of information technologies and typifies this historic surge in global IT development. Delaying 5G development purely on the basis of security risks is not reasonable. Rather, we must persist in viewing security risks from the perspective of development, properly handle the relationship between development and security, and ensure that the two advances in parallel. With a more flexible security protection mechanism than 4G, 5G is able to provide more powerful communication security capabilities. A

virtuous circle of "risk-response-new risk-new response" will be established. 3GPP will continue to enhance the security[4] in response to emerging attacks and security threats and achieve the coordinated advancement of both 5G security and development.

2. Looking at 5G security from a system perspective. Information technologies are changing at an ever-increasing rate. The previously decentralized and independent networks are now becoming highly interconnected and interdependent. 5G technology is integrating with and penetrating various fields, and security risks are closely linked with different entities. Facing such risks, it is necessary to view and address 5G comprehensively from a system perspective. 5G technology developments and related application scenarios are extensive, open, challenging, and diverse. Against this backdrop, it is necessary to clarify the responsibilities and obligations of different entities in various links of the industry chain, such as network operators, equipment suppliers, and industry application service providers. However, it must be noted that the responsibilities of a single link should not be stressed or magnified excessively. It is also necessary to strengthen the cooperation and coordination between various entities, allow governments, standardization organizations, enterprises, research institutions, and users to take initiative, clarify the security responsibilities of all parties, and build a 5G security governance system in which multiple entities participate.

3. Looking at 5G security from an objective perspective. Every network technology has its own security risks and vulnerablilities, and 5G network is no exception. The best way to address such risks is by analyzing and viewing them from an objective perspective. As 5G integrates with new technologies and applications such as IoT and AI, more complex security challenges will surely emerge. Such challenges can only be effectively overcome by conducting a comprehensive assessment of 5G security risks from an objective and neutral technical perspective. 5G security risks can be gradually resolved through industrial innovation and technological R&D based on mature mechanisms and technical response measures that already exist. Magnifying, complicating, or even politicizing security issues of a technical nature, labeling enterprises with different tags, or taking non-market approaches, will in no way contribute to the effective resolution of 5G security issues.

[4]3GPP: the reassessment of other security threats such as replay, bidding down, man-in-the-middle and inter-operator security issues have also been taken into account for 5G so as to further enhance 5G security. https://www.3gpp.org/news-events/1975-sec_5g

4. Looking at 5G security from a cooperation perspective. Countries may vary in terms of their conditions, stage of network development, or actual challenges faced, but when it comes to addressing security risk challenges and the need to strengthen governance of cybersecurity space, most countries are on the same page. On the whole, the international community is increasingly accepting the idea that we are all in the same boat, and we all share the same future. Likewise, 5G security is a global challenge that no country is free from. We have moved on from having multiple standards in the past to today's global unified standards typified by 5G, and the 5G process is a prime example of what can be achieved by innovating through cooperation among countries. In the field of security, countries should also work together to strengthen innovation through cooperation and jointly build a peaceful, secure, open, and cooperative cyberspace.

IV. 5G Security Analysis

5G represents not only a technological change, but also the emergence of a new ecosystem. Given this, understanding 5G security issues requires both an objective analysis from the perspective of technology and scenarios, and a comprehensive assessment from the perspective of the industry ecosystem as a whole.

1. Security analysis of 5G key technologies

(1) Network Function Virtualization (NFV)

Security risks. 1. In a virtual environment, management and control functions are highly centralized, which means the safe and stable operation of the entire system will be jeopardized if the functions fail or are illegally controlled; 2. Multiple virtual network functions (VNFs) share the same underlying infrastructure resources, and therefore an attack on one virtual network function will also affect other functions; 3. Due to the adoption of a large amount of open source and third-party software in network virtualization, the possibility of security vulnerabilities being introduced is increasing[5].

Technical countermeasures. The above risks can be countered by referring to the existing cloud security solutions used in 4G core networks and IT industry applications, as well as to the network virtualization security standards

[5] ENISA "Threat Landscape of 5G Networks", Nov. 2019

formulated by the European Telecommunications Standardization Institute (ETSI) [6]. The specific countermeasures are as follows: 1. Reinforce the security of the system, track and audit the operations of management and control, and ultimately improve the ability to prevent attacks; 2. Provide end-to-end, multi-layered resource and security isolation measures, and encrypt and back up key data; 3. Strengthen the security management of open source third-party software.

(2) Network Slicing

Security risks. Network slicing leverages virtualization technology to logically isolate shared resources. Without appropriate security isolation mechanisms and measures in place, an attacker can target a network slice with a low level of security protection and use it as a springboard to attack other slices[7], thereby affecting their normal operations.

Technical countermeasures.1. Use cloud-based and virtualization isolation measures, such as physical isolation, virtual machine (VM) resource isolation, and virtual firewalls; 2. Achieve accurate and flexible slice isolation, ensuring resources are effectively isolated between users on different slices; 3. Properly manage the operation and maintenance (O&M) of network slices and operation security, and ensure that the corresponding technical measures are implemented.

(3) Edge Computing

Security risks. 1. Edge computing nodes have moved to the edge of the core network. This leaves them more vulnerable to physical attacks if deployed in a relatively insecure physical environment; 2. The edge computing platform can have multiple applications deployed that share related resources. If an application is breached due to insufficient protection, other applications on the edge computing platform will also be compromised.

Technical countermeasures. 1. Provide physical protection and network protection for edge computing facilities, make full use of existing security technologies to strengthen the platform, and enhance the anti-theft and damage-resistant measures of edge facilities; 2. Strengthen application

[6] NFV security series specification, https://www.etsi.org/deliver/etsi_gs/NFV-SEC/
[7] "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks Report", NIS Cooperation Group, Oct. 2019.

security protection and improve the security authentication and authorization mechanism for access of edge computing nodes from the application layer. When third-party applications are deployed, it is necessary to clearly define the security responsibilities of all parties according to the deployment model and implement them collaboratively.

(4) Network Capability Exposure

Security risks. 1. NCE may enable some services and/or network related data to be shared instead of be protected on a network operator's internal closed platform. This weakens the network operator's ability to manage and control data to some extent; 2. The NCE interface adopts the common Internet protocols, which makes the existing security risks of the Internet a further threat to 5G networks.

Technical countermeasures. 1. Strengthen protection of 5G network data and enhance monitoring and handling of security threats. 2. Strengthen the security protection capabilities of the NCE interface and prevent attackers from using the open interface to penetrate the operator's network.

Overall, although key technologies such as NFV, network slicing, edge computing, and NCE introduced by 5G networks have brought some new security threats and risks, there are higher requirements on data protection, security protection, operation, and deployment. However, the introduction of these new technologies is also a gradual process of continuous iteration. The associated security risks can be mitigated and addressed through enhanced security protection measures, such as ex-ante risk assessment and appropriate technical solutions and security measures during and after the events.

2. Security analysis of typical 5G scenarios

5G application scenarios face new security risks due to the technology used and the characteristics of the specific application scenario, and this has become a key factor affecting the development of 5G convergence services. At present, the most typical 5G scenario is eMBB, which has been gradually expanded to vertical industries. For this scenario, 3GPP has already completed the development of related security standards, while the standards for uRLLC and mMTC scenarios are still under development.

eMBB scenario. In this scenario, the main applications include 4K/8K ultra-high-definition mobile video and immersive augmented reality (AR)/virtual reality (VR) services. Such applications produce huge volumes of traffic, which poses challenges on existing network security protection methods. Also, significantly increased data traffic at the edge of the network is expected with the arrival of 5G, which has 10 times the data rate of 4G. The huge traffic volumes will make it extremely difficult for security devices — such as firewalls and intrusion detection systems deployed in existing networks — to ensure adequate security protection when it comes to traffic detection, radio coverage, and data storage.

uRLLC scenario. Typical applications include the Industrial Internet and the Internet of Vehicles (IoV) for autonomous driving, applications that require the ultra-reliability, low-latency service quality assurance provided by uRLLC. This requirement for low-latency will actually constrain the deployment of complex security mechanisms, posing security risks. The deployment of security mechanisms, such as access authentication, data transmission security protection, device switchover on the move, and data encryption and decryption, will increase the latency. In short, overly complex security mechanisms are not suitable for scenarios with low-latency services.

mMTC scenario. This scenario is characterized by wide coverage of applications, large numbers of access devices, scattered application regions, equipment suppliers with differing standards, and numerous business types. Such a large number of devices of varying types are vulnerable to attacks, which threatens the security of network operations. In the 5G era, there will be vast numbers of IoT devices accessing 5G networks, with the number of global connected IoT devices expected to reach 25.2 billion by 2025[8]. With limited computing and storage resources, it would be difficult to deploy complex security policies on such a large number of low-power devices. Once attacked and used to form a device botnet, these devices will then become the sources of attack, triggering network attacks on user applications and backend systems and posing network risks, such as network interruptions and system crashes[9].

In response to the security risks of typical 5G application scenarios, the following countermeasures can be taken: 1. Strengthen the evolution and

[8] GSMA research report, "IoT: The next wave of connectivity and services" https://www.gsmaintelligence.com/research/2018/04/iot-the-next-wave-of-connectivity-and-services/665/

[9] "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks Report", NIS Cooperation Group, Oct. 2019.

upgrading of security protection technologies and equipment, and effectively adapt and respond to the impact that massive volumes of traffic have on existing protection methods; 2. Establish a security mechanism that can meet low-latency requirements, optimize the latency generated by access authentication, data encryption and decryption, etc., and strive to improve security protection capabilities under low-latency conditions; 3. Build a security model based on mMTC, establish an intelligent dynamic defense system to respond to network attacks, and prevent the horizontal spread of network security threats.

3. Security analysis of 5G industry ecosystem

The main stakeholders in the 5G industry ecosystem are network operators, equipment suppliers, and industry application service providers. Their continuous innovation and global cooperation in basic security technologies and industry support capabilities is critical to the enhancement of 5G security.

(1) Security analysis of network deployment and operation. Security management runs through the entire lifecycle of 5G network deployment and operation. As such, network operators should take appropriate measures to manage the following security risks and ensure the continuity of services provided by their networks: 1. In terms of 5G security design, because 5G networks are especially open and complex, there are higher requirements placed on access management, security domain division and isolation, internal risk assessment and control, and emergency response; 2. In terms of 5G network deployment, because the network elements are relatively distributed, it is difficult to ensure proper system configuration and sufficient protection of the physical environment; 3. In terms of O&M, 5G O&M features fine granularity and multiple roles. Such features, however, increase the risk of incorrect O&M configuration, which lead to security attacks that may otherwise have been avoided. In addition, 5G's high requirements on O&M pose challenges to operational compliance and professional capabilities of the practitioners, and affect the security of 5G networks.

(2) Analysis of application security in vertical industries. 5G is deeply integrated with vertical industries, and the security of the 5G industry ecosystem is largely influenced by industry application service providers, as well as network operators and equipment suppliers, in the following ways: 1. In terms of security, 5G networks, applications, and devices are deeply intertwined. As industry application service providers deliver services directly to users, they assume the primary responsibility for ensuring application and

device security. It is also their duty to clarify the security responsibility boundaries with network operators, strengthen collaboration and coordination with them, and solve security issues from a holistic perspective; 2. Different vertical industries have different applications, each with varying demands and capabilities when it comes to security. This makes it unfeasible for a single security solution to ensure application security in every vertical industry.

(3) Analysis of supply chain security. 5G technology has high skill requirements, a wide range of applications, and a long industry chain that covers system equipment, chips, devices, application software, operating systems, and many more. The healthy development of 5G and its applications rely on the continuous innovation and global cooperation of the basic security technologies and industry support capabilities of the entire industry chain. Failing to strengthen innovation in fundamental, general, and forward-looking security technologies, as well as the various links of the industry chain, will prevent us from updating and improving 5G network security products and solutions at the same time. It will also hinder us from providing more secure and reliable 5G products, thereby increasing the vulnerabilities of network infrastructure and preventing the enhancement of 5G security systems.

The 5G network ecosystem is comprised of numerous players, each with different roles. This calls for the different levels of security responsibilities and requirements of these various entities to be fully considered in the 5G network ecosystem. Security measures and protection must be considered from the perspective of network operators and equipment suppliers, and application service providers in energy, finance, health, transportation, industrial sectors, and other industries must also take appropriate security measures.

V. 5G Security Train of Thoughts and Measures

To properly handle 5G security issues, we can build on the existing 4G security management framework and technical support measures and take targeted measures to address new security risks and uncertainties.

1. Adhere to the simultaneous deployment of development and security. We should adhere to the concept of placing equal emphasis on development and security, paying equal attention to both encouragement and regulation. At the same time as accelerating 5G network deployment and deepening 5G converged applications in various fields, we should continue to build 5G security capabilities, and take a holistic and coordinated approach towards the security of 5G network facilities, applications, and data. We must also closely monitor 5G security risks, dynamically conduct 5G technology security assessments, and identify the priorities of 5G security protection.

2. Establish a security responsibility system that coordinates and clearly defines the responsibilities of multiple parties. We must clarify the responsibilities of different parties in the industry ecosystem, and continuously improve relevant laws, regulations, policies, and requirements in relation to areas such as personal information protection, critical information infrastructure protection, and network information governance. Also, network operators, equipment suppliers, industry service providers, and other entities must assume their respective roles and responsibilities. We must also strengthen the coordination between various industries, bring industry organizations into play, establish and improve the security service protection standards and credit systems for 5G networks and vertical industries, and jointly address the security issues of the converged applications of 5G in vertical fields.

3. Continue to promote the development of 5G security innovation. We must strengthen the research on 5G security technologies and standards, accelerate the establishment of 5G security evaluation systems, promote the evolution and upgrading of network security products in areas such as asset identification, vulnerability mining, intrusion prevention, data protection, track and traceability, and continue to build a comprehensive, diverse, and reliable 5G security product supply and service system. We should also accelerate the commercialization and pilot verification of 5G security technology innovations, and increase the promotion of security services and solutions in vertical fields such as Internet of Vehicles and the industrial Internet.

4. Strengthen the dynamic assessment of security risks in 5G applications. The converged applications of 5G in various vertical industries will continue to emerge as networks are deployed on a larger scale. The characteristics of these applications are highly related to vertical fields, and security risks also continuously and dynamically change. Therefore, when studying standards related to industry application security, the respective characteristics of 5G vertical fields must be fully considered. We must continue to assess security risks across industries and domains, strengthen the application and transformation of evaluation results, and promptly propose security response and handling measures to effectively mitigate security risks.

5. Build an integrated 5G network security protection mechanism. We should actively develop a means by which the security of 5G network infrastructure is ensured, establish and improve the mechanism for sharing and interconnecting 5G network threat information, and realize threat information sharing and co-governance. We should also accelerate the construction of an integrated 5G network security defense system that integrates threat monitoring, global awareness, early warning & protection, and coordinated handling, thereby forming a comprehensive network security protection capability.

6. Strengthen the cultivation and training of talents with all-round 5G capabilities. Promote the training of 5G interdisciplinary professionals, establish and improve the talent training system featuring industry-education integration and university-enterprise cooperation, increase support for talent training, continue to deepen 5G security training and education, enrich the 5G security talent discovery mechanism, and establish multiple ways to select security practitioners.

VI. Outlook and Initiatives

When it comes to the development of 5G, countries have common concerns as well as varying requirements. It is critical that countries seek common goals and meet common challenges while respecting each other's core interests, so that 5G technology can better benefit the whole world. We call on all parties to uphold the concept of cooperation and mutual trust, accelerate the formulation of international standards for 5G security, establish an evaluation and certification system based on mutual trust and recognition, strengthen the upstream and downstream cooperation in the industry, and ultimately increase confidence in global 5G security development.

1. Strengthen open cooperation and mutual trust, and work together to address 5G security risks. We must adhere to the concepts and principles of openness, inclusiveness, equality, mutual benefit, and win-win cooperation, promote the establishment of a bilateral or multilateral framework that enhances mutual trust, pay full attention to 5G security concerns of all parties, and actively discuss 5G security-related international policies and rules within the framework of multilateral organizations such as the International Telecommunication Union — a specialized agency of the United Nations. We should also enhance strategic mutual trust of all parties, further improve the dialogue and negotiation mechanism, strengthen the sharing of information on 5G network threats, and effectively coordinate and handle major network security incidents. Finally, we should explore best practices and share advanced experiences and practices in responding to 5G security risks.

2. Accelerate the promotion of international standards for 5G security and form a global consensus. Under the framework of 5G international standardization bodies — such as ITU and 3GPP — we must focus on new or enhanced key technologies in 5G networks, such as NFV and network slicing. As well as this, we should jointly promote the development of subsequent international standards for 5G enhanced technologies and security mechanisms, accelerate the formation of 5G security solutions covering multiple application scenarios. It is also critical that we strengthen the development of product and service security systems, and strictly follow international security standards and specifications throughout the entire lifecycle of 5G, from product design to R&D and O&M.

3. Establish an international 5G security evaluation and certification system to promote mutual trust and recognition. It is vital that we strengthen communication and cooperation, promote the formation of a 5G security evaluation and certification system based on a global consensus, build a security audit and technical security testing mechanism covering the entire process from product R&D and design to manufacturing and O&M, and accelerate the formation of an open, transparent, widely-accepted 5G security trust baseline and security evaluation grading system. We must also promote the bilateral or multilateral mutual recognition of evaluation results, and jointly ensure the healthy development of the 5G global industry chain.

4. Strengthen the upstream and downstream cooperation of the industry chain and boost confidence in 5G security. We should strengthen collaboration and innovation of the global mobile communications industry

chain, actively build global industry application cooperation and innovation platforms, increase global cooperation on the innovation and research of key components, core algorithms and other aspects, and promote the demonstration, cooperation, and sharing of best practices and experience in diversified applications on 5G networks. Additionally, we must encourage diversified global procurement strategies, promote the formation of an efficient global industry chain with reasonable allocation and division of labor, promote the connectivity of mobile communication supply chain, and gradually connect various production factors in the upstream and downstream supply chains in various regions and around the world. Finally, we must create an open, fair, transparent, and non-discriminatory market environment for the global development of the 5G industry.