http://fddi.fudan.edu.cn

复旦智库
THINK TANKS FUDAN

FUDAN REPORT SERIES

2020 no.8(31)

PIONEER INSIGHT

Report on the Cybersecurity Legislation of Major European Countries

Fudan Development Institute
Cyberspace International Governance Research Institute in Fudan University
China Institute for Cyberspace Strategy at Fudan University

Report on the Cybersecurity Legislation of Major European Countries

Jiang Tianjiao, Shen Yi

Fudan Development Institute

Cyberspace International Governance Research Institute at Fudan University

China Institute for Cyberspace Strategy at Fudan University

October 15, 2020

Authors

Project Head:

Shen Yi, Professor at Fudan Development Institute, Director of the Fudan University Cyberspace International Governance Research Institute

Project Deputy Head:

Jiang Tianjiao, Assistant Professor at Fudan Development Institute, Assistant to the Director of the Fudan University Cyberspace International Governance Research Institute

Project Members:

Lei Ting, Research Assistant at the Fudan University China Institute for Cyberspace Strategy

Lu Bin, Research Assistant at the Fudan University China Institute for Cyberspace Strategy

Zhu Jiahao, Research Assistant at the Fudan University China Institute for Cyberspace Strategy

Gao Yu, Doctoral student at the Fudan University School of International Relations and Public Affairs

Gong Yunmu, Doctoral student at the Fudan University School of International Relations and Public Affairs

Contents

Introduction i
1. Panorama of 5G Networks in Europe 1
1.1 Overview of 5G in Europe 1
1.2 Policy Regulation – Access Criteria Assessment Quadrant 2
2. Legislation Trends and Evolution 5
2.1 Digital Economy Strategy and Cybersecurity Legislation in Europe 5
2.2 European 5G-Related Strategic Documents and Security Toolbox 7
2.3 Trends in AI Legislation 8
3. Analysis of Key National Legislation 10
3.1 Overview of Key National Legislation 10
3.1.1 Germany 14
3.1.2 France 19
3.1.3 Italy 21
3.1.4 Spain 26
3.1.5 United Kingdom 30
3.1.6 Finland 32
3.1.7 Denmark 33
3.1.8 Sweden 38
3.1.9 Poland 39
3.1.10 Estonia 42
3.1.11 Russia 47
3.2 Examples of "Good Law" and Analysis of Core Clauses 50
3.3 Examples of "Bad Law" and Analysis of Core Clauses 51
3.4 Analysis of the Difference Between "Good" and "Bad" 53
4. Conclusion 55

Introduction

As important cyberspace actors, China and Europe are key to building a global governance system in cyberspace. China is the fastest-growing newcomer in cyberspace, while Europe has the highest Internet penetration rate and is actively promoting the construction of a digital single market. Studying European cyber legislation is not only greatly significant in terms of enhancing China-EU cyber cooperation, but also can shed some light on how to develop a benign cyberspace interaction model among the major world powers.

However, China and Europe still face challenges regarding the formation of a network order, a lack of trust, and strategic suspicion, creating a cybersecurity dilemma on multiple levels, including international, bilateral, and domestic.

Realistically, China and the EU share common interests in these areas, despite inevitable differences. Based on practical and rational considerations, China and the EU should cooperate and compete when dealing with the international governance of cyberspace. The lack of trust between the two sides mainly manifests itself in the lack of dialogue surrounding the importance of cybersecurity to China-EU relations, the lack of results and practical cooperation, and a failure to fully utilize the potential role of online dialogue in enhancing trust, dispelling misunderstandings, and strengthening cooperation.

Moreover, considering factors associated with the international environment, such as external pressure, China and Europe have actively or passively become part of a wider confrontation between Western countries and emerging economies in almost all areas of cyberspace governance.

Countries represented by Germany create legislation and policies based on objective criteria such as technical attributes. Targeted laws and regulations are vital for information security and cybersecurity control. Examples of these are amendments to existing laws or separate legislation to combat information crimes; setting certification standards and trusted parameters, and introducing additional technical requirements to regulate equipment deployment.

Countries such as the UK typically make decisions based on ideology. However, the "negative spillover effect" of US network policy has already brought political risks. Some countries try to use country-of-origin as a market access indicator for political repression and other such purposes.

In this context, the game between countries will lead to unfair competition in the 5G market. An independent and rational Europe could be a blessing for the whole world.

1.Panorama of 5G Networks in Europe

1.1 Overview of 5G in Europe

Europe has the highest level of network informatization of any region in the world, and it is also an important market for the commercial construction of future 5G networks. In July this year, IDATE DigiWorld, a European digital economy think tank released the"5G Observatory Quarterly Report (Up to June 2020)". This report stated that 13 EU member states, namely Austria, Belgium, Finland, Germany, Hungary, Ireland, Italy, Latvia, the Netherlands, Poland, Romania, Spain, and Sweden, in addition to the UK have deployed 5G commercial equipment.

Figure 1: 5G Commercial Services in 14 European Countries

Source: IDATE DigiWorld[1]

The progress of 5G market development in different European countries also varies. As shown in Figure 1, the 27 EU member states and the UK have conducted a combined total of 192 5G trials within their cities. Five of these, namely Spain, Germany, Italy, France, and the UK, are among the countries worldwide to have held the most successful 5G trials. The goal of the 5G Action Plan adopted by the European Commission in 2016, is to ensure that the commercial promotion of 5G is achieved in at least one major city of each member state by the end of 2020, and in all urban areas and cities by 2025. This plan also targets uninterrupted 5G coverage for major land transportation routes. The 5G Action Plan was approved by the EU member states in 2017. Over the next five years, European countries will accelerate 5G commercial deployment, while the importance of the regional market is self-evident.

At the national level, 11 EU member states (Finland, Sweden, Estonia, Denmark, the Netherlands, Germany, the Czech Republic, Luxembourg, Austria, France and Spain), as well as the UK, have published 5G roadmaps. Within the EU, only four member states – Hungary, Ireland, Italy and Latvia – are yet to publish a national strategy for 5G.

[1] *5G Observatory Quarterly Report (Up to June 2020)*, IDATE DigiWorld, July, 2020 http://5gobservatory.eu/wp-content/uploads/2020/07/90013-5G-Observatory-Quarterly-report-8_1507.pdf.

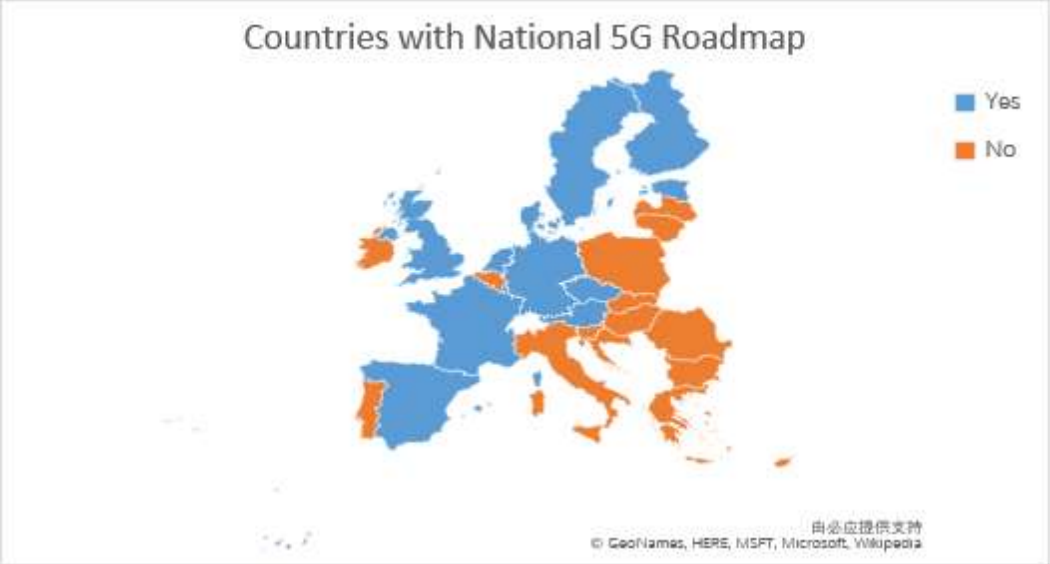

Figure 2: 5G Roadmaps Across Europe

Source 2: IDATE DigiWorld[2]

1.2 Policy Regulation – Access Criteria Assessment Quadrant

In order to provide a comprehensive and accurate assessment of the cybersecurity of 5G networks and vendor access in key European countries, we have examined the legislative status of each country and compiled a set of procedures for judgment and evaluation.

[2] *5G Observatory Quarterly Report (Up to June 2020)*, IDATE DigiWorld, July, 2020 http://5gobservatory.eu/wp-content/uploads/2020/07/90013-5G-Observatory-Quarterly-report-8_1507.pdf.

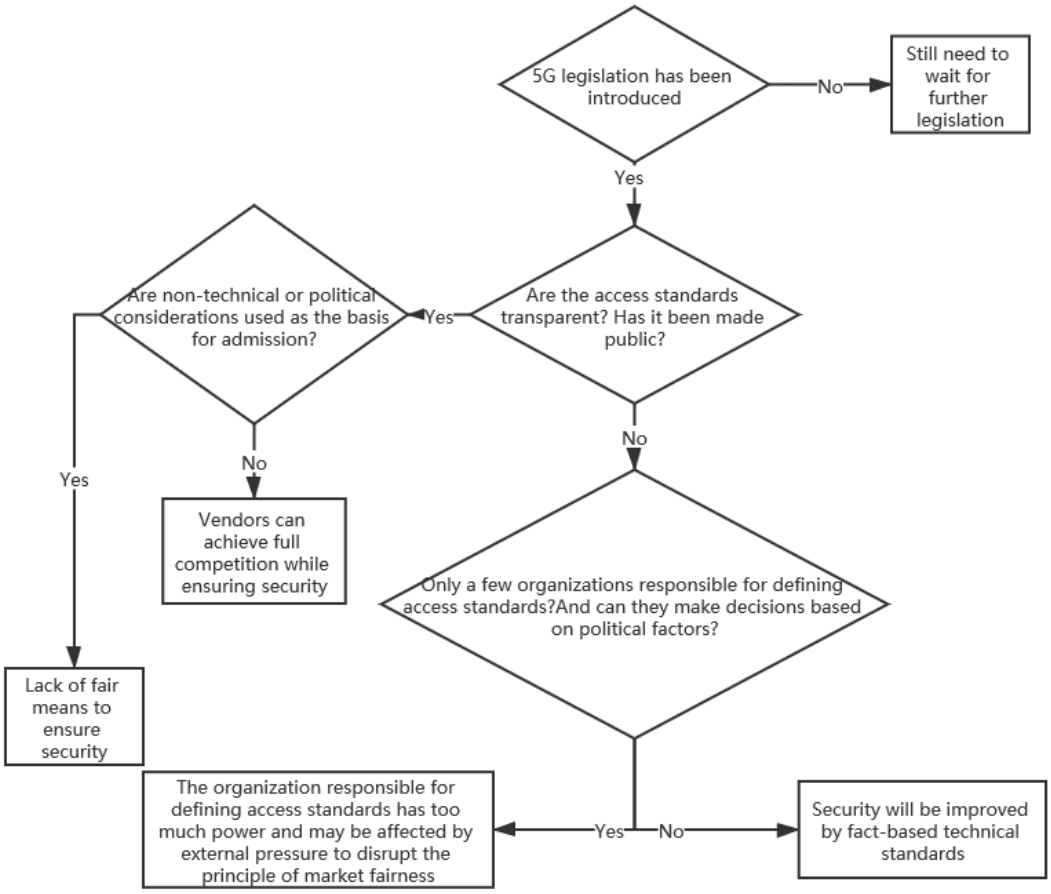

Figure 3: Policies and Regulations – Access Standard Evaluation Process

During this process, we focus on answering a number of questions, including whether there is effective 5G legislation, whether access standards are clear and transparent, and whether the designated organization has the complete authority to make the final assessment. The most important thing is whether the formulation of future standards and regulations will or may involve political considerations that are unrelated to technical factors. We hope to evaluate each country's position and tendency towards establishing a fair and secure 5G market in light of their different domestic situations.

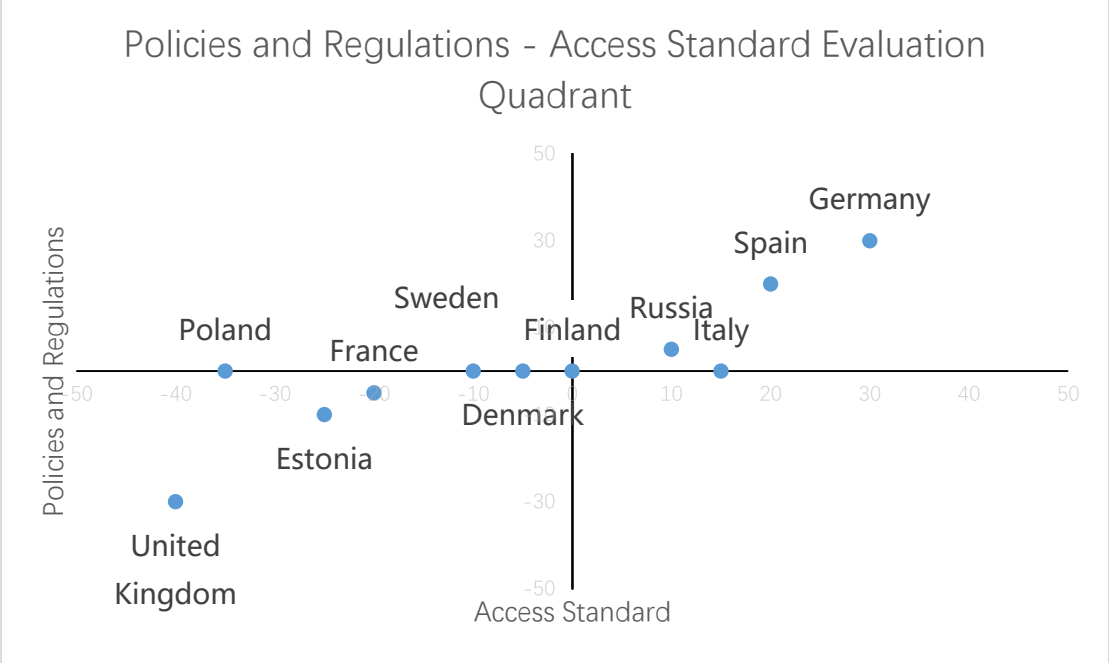

Figure 4: Policies and Regulations – Access Standard Evaluation Quadrant

Finally, we mapped the 5G policies and regulations of various countries in the same coordinate system, and obtained the "National Policies and Regulations – Access Standard Evaluation Quadrant" for each country, as shown above. The top-right quadrant represents the country's willingness to adopt an open and positive attitude to ensure and improve 5G security by setting objective standards. A typical example is Germany. In response to the requirements of Section 109 of the Telecommunications Act, Germany has revised its security requirements, adding key basic component certification requirements, specific regulatory compliance requirements, supplier share requirements, etc. However, it has not addressed the access requirements for specific manufacturers. Countries in the bottom-left quadrant exclude some manufacturers from 5G construction through administrative regulations and standards, giving corresponding agencies freedom within legislation, and setting a threshold based on political factors as part of security audits. In the UK, for example, NCSC, a single agency, makes the final decision on manufacturers. A "home country" restriction is part of the identification criteria, classifying manufacturers from a particular country as high-risk. Under external pressure, the UK also prevents individual manufacturers from participating in 5G construction.

Many countries within the quadrant chart have access standards are at the same level. Most of these countries have introduced legislation that grants government departments the authority to exclude individual manufacturers, but the exclusion criteria have not yet been determined or announced. This means these countries still have time to make decisions that will embrace open markets.

2.Legislation Trends and Evolution

Historically, Europe has been the leader in cybersecurity legislation. In 1981, the member states of the European Council signed the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", known as the Strasbourg Convention. Germany passed the "Information and Communication Services Regulation Act" in 1997, which was the world's first Internet regulatory law. In 2001, the EU initiated and agreed the world's first international treaty against cybercrime, the "Convention on Cybercrime" known as the Budapest Convention.

2.1 Digital Economy Strategy and Cybersecurity Legislation in Europe

2013	•"Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"
2015	•"A Digital Single Market Strategy for Europe"
2016	•"General Data Protection Regulation" •"Directive on Security of Network & Information Systems" (NIS Directive) •"5G for Europe: An Action Plan"
2019	•"EU Cybersecurity Act" •EU Commission "the Commission Recommendation: Cybersecurity of 5G Networks" •ENISA "Therat Landspace for 5G Networks" •EU Commission "Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G "
2020	•"Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures" •"Secure 5G Deployment in the EU - Implementing the EU Toolbox" •"A European Strategy for Data" •WHITE PAPER "On Artificial Intelligence - A European Approach to Excellence and Trust"

Table 1: EU Legislation and Strategic Documents Related to Cyber Security and 5G Construction

Benefiting from the advantages of a single market and huge number of consumers, the EU can formulate laws and regulations to regulate the global market and develop into a global regulatory power. In 2015, the European Commission introduced the "European Digital Single Market Strategy", which aims to maintain Europe's leading role in the development of the world's digital economy by successfully building a digital single market. This strategy also intends to ensure that the scale of the single market serves consumers and enterprises. In 2020, the European Commission launched the "European Digital Strategy", which proposes strategic ideas in four areas: Sharpening policy tools, "hunting" technology giants, strengthening facility connectivity, and promoting digital environmental protection. This

strategy intends to make the EU the world's safest, most attractive, and most dynamic digital economy, and strengthen the digital skills of EU enterprises and citizens. Realizing these digital economy development goals will require the protection of relevant laws and regulations.

The EU's General Data Protection Regulation (GDPR), adopted on April 27, 2016, came into effect on May 25, 2018. These regulations expand the scope to include companies from outside of the EU, provided that the company is established within the EU or the company conducts data processing activities that are related to individuals in the EU, provisions goods and services to individuals in the EU, or monitors the behavior of individuals within the EU. According to the above regulations, all companies that provide services to individuals in the EU are subject to these regulations. As a result, the European Union, supported by a huge consumer market, exercises its regulatory powers in market supervision, and then exports EU standards to the global market, in what is known as the "Brussels effect."

In addition to protecting personal data, the EU has taken relevant measures to ensure cybersecurity. In 2013, the European Union issued its first comprehensive cybersecurity policy document, the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". The strategy laid out in this document focuses on EU policies and measures for addressing cyber threats and security risks, establishes guiding principles for EU cybersecurity governance, and sets strategic goals for the establishment of an "open, free and secure" cyberspace. In addition, it led to the formation of the EU Cyber Defense Policy Framework.

The European Union passed the Cybersecurity Act in 2019, officially introducing cybersecurity legislation. The act also established a general European cybersecurity certification framework. The purpose of this is to improve the operating conditions of the single market by enhancing the level of cybersecurity within the EU, and unifying the cybersecurity certification systems of member states. The subject and scope of the European cybersecurity certification system include the types or categories of information and communication technology (ICT) products, ICT services and ICT processes. A unified certification system at EU level helps to reduce gaps between member states in terms of cyber security, enhance consumer confidence in products that have passed the relevant certifications, and promote the comprehensive development of the EU single market.

As part of the Cybersecurity Act, the European Union Agency for Cybersecurity (ENISA) has been created as a permanent EU cybersecurity agency. The primary goal of ENISA is to establish European cybersecurity certification schemes that ensure cyber security protection for ICT products, services, and processes within the EU, while preventing the fragmentation of the internal market. ENISA shall actively support the activities of EU member states, EU institutions, and groups and offices to improve cybersecurity and offer member states professional knowledge and suggestions for reference. As a result, ENISA has become an important actor in maintaining the EU's cybersecurity and elements of the EU's 5G strategy, such as coordinating member states to complete 5G network security risk assessments and publishing the "Threat Landscape for 5G Networks".

2.2 European 5G-Related Strategic Documents and Security Toolbox

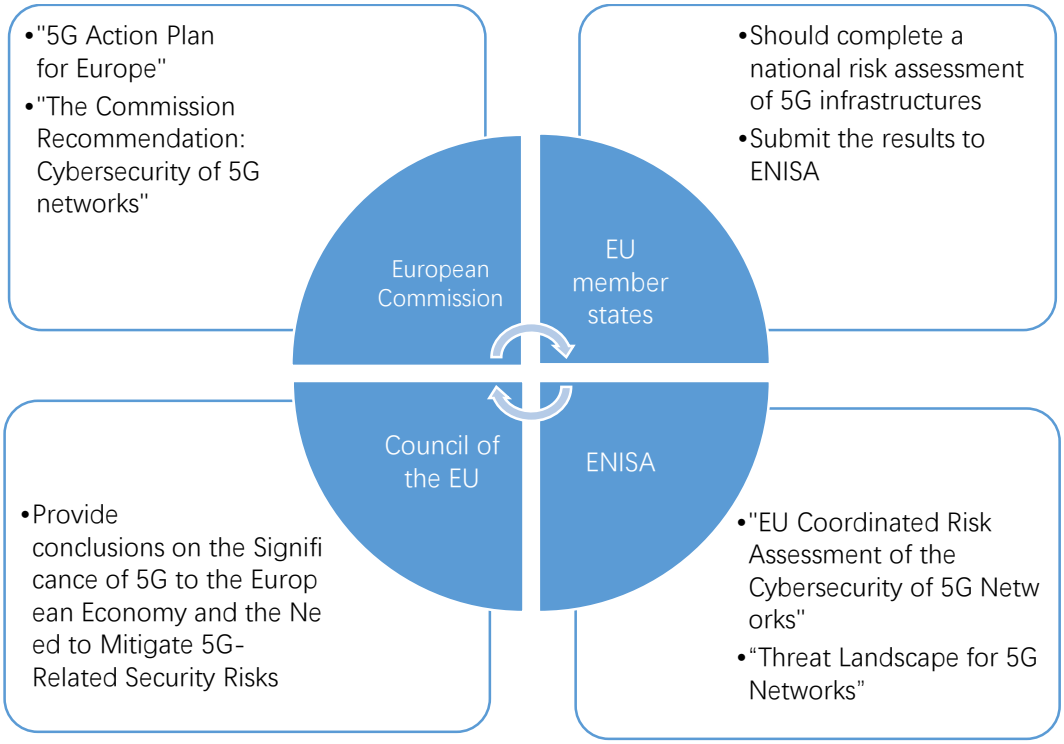

Table 2: Main Actors in the EU's 5G Strategy

On September 14, 2016, the European Commission launched the "5G Action Plan for Europe", setting the timetable for 5G deployment: Testing was to begin in 2017, with a roadmap for 5G deployment in various countries being completed by the end of the year; pre-commercial testing in 2018; 5G services to start launching in all EU Member States by the end of 2020 at the latest, followed by rapid construction to ensure uninterrupted 5G coverage in urban areas and along main transport paths by 2025. On March 26, 2019, the European Commission issued "The Commission Recommendation: Cybersecurity of 5G networks" and called on all Member States to complete national risk assessment and review measures, coordinate risk assessments at EU level, and prepare a toolbox of possible risk reduction measures.

After the Member States completed their 5G network infrastructure risk assessments, ENISA released the "EU coordinated risk assessment of the cybersecurity of 5G networks" on October 9, 2019. This report analyzes the security risks of the EU's 5G network in terms of threat types, threat actors, assets, vulnerabilities and risk scenarios. Among them, two major security risks originate from suppliers. The first is the possibility of suppliers being interfered with by non-EU countries. This could include suppliers having close ties with governments of non-EU countries, the non-EU country lacking the relevant legislation to achieve democratic checks and balances, or the non-EU country failing to sign security or data protection agreements with the EU. Second, is the risk of relying too heavily on a single supplier, leading to a lack of diversity in both equipment and solutions. In addition, the report focuses on the country where the supplier is headquartered. For example, the report identifies Ericsson and Nokia as suppliers that are headquartered in the European Union, while identifying other suppliers as being headquartered outside the EU. According to the report, the corporate governance applicable to these two types of suppliers has notable differences, for example in

terms of level of transparency and the type of corporate ownership structure. The report classifies suppliers based on "EU" and "non-EU" standards, and emphasizes the potential security risks of non-EU suppliers. This reflects the EU's consideration of geopolitical factors during the construction of 5G networks.

On January 29, 2020, the European Commission issued the "Secure 5G deployment in the EU – Implementing the EU toolbox", stipulating that all member states must develop measures for appropriately dealing with current and future 5G network security risks. These measures include restricting or prohibiting certain 5G equipment or setting specific requirements and conditions for the supply, deployment and operation of 5G equipment. Specifically, EU member states must be able to effectively assess the risks of suppliers and prevent any high-risk suppliers from being involved with critical or sensitive assets. Core network functions, network management and orchestration functions, and access network functions are all examples of sensitive assets. In addition, each member state should ensure that operators have appropriate multi-vendor strategies to avoid or limit major dependency on a single supplier (or suppliers with similar risk profiles), ensure an adequate balance of suppliers at national level, and avoid dependency on suppliers considered to be high risk.

The EU Toolbox introduced the concept of "high risk suppliers". Member states are required to take measures that prevent high-risk suppliers from participating in key or sensitive network core functions. The Toolbox does not identify high-risk suppliers, but emphasizes the need to conduct supplier risk assessments based on security measures and objective standards. In addition to corresponding technical measures, member states have increased their consideration of non-technical factors within security risk assessments. The European Commission is committed to providing necessary support for member states to adopt relevant strategic measures that will protect the EU's technological sovereignty and ensure the EU maintains its leading position in related fields, such as cybersecurity technology.

A pressing issue for the EU is how to maintain a fair and non-discriminatory market environment while protecting the cybersecurity of 5G. The current division of "EU suppliers" and "non-EU suppliers" and the concept of "high-risk suppliers" constitute a certain level of market access discrimination against suppliers from outside the EU. The EU institutions and member states have given this discrimination legitimacy by emphasizing "security". However, national security must be reasonably controlled, and the EU must prevent member states from simply using security as a reason for decisions. For example, the governments of member states may use "high security risks" as an excuse to exclude specific manufacturers and protect the interests of domestic enterprises or other related "critical and sensitive" industries. This could even take the form of administrative measures, such as setting non-technical standards. Such actions would greatly damage the free flow of goods and capital within the EU's single market and weaken the EU's credibility as a global regulatory force.

In these documents, the European Commission mentions that non-EU countries may exert influence on member states by interfering with specific suppliers, and that the links between suppliers and non-EU countries could constitute potential security risks. In fact, the influence of non-EU countries on the construction of the EU's 5G network does not only come from equipment suppliers. Cooperation between the United States and Eastern European countries is a typical example.

2.3 Trends in AI Legislation

In terms of AI-related legislation, most governments are currently adopting a "wait and see" approach towards laws and regulations on AI, and there are more guidelines than real laws. However, in the coming years, we expect regulatory measures to gradually penetrate various AI applications. Through the continuous integration of "5G + AI" technology, third

parties will find it easier to collect, transmit, access, and share personal data. Accordingly, the chances of personal data being violated will increase.

According to the report "Worldwide AI Laws and Regulations 2020" released by Cognilytica Research in February 2020, the European Union is the most active body in terms of proposing new rules and regulations, with existing or proposed EU rules existing in seven out of nine categories (facial recognition and computer vision, autonomous vehicles, AI-relevant data privacy, conversational systems and chatbots, lethal autonomous weapons systems [LAWS], AI ethics and bias, AI-supported decision making, malicious use of AI, and general use of AI) of areas where regulation might be applicable to AI (no legislative moves regarding conversational systems & chatbots and malicious use of AI).

For example, findings from the report show that 24 countries and regions have established permissive laws for autonomous vehicle operations, and eight more are currently in discussions to enable the operation of autonomous vehicles. Many European countries such as Belgium, Estonia, Germany, Finland, and Hungary have laws in place that allow for the testing of autonomous vehicles on their roads. France has expressed an ambition to assume a major role in the development of autonomous vehicles, with an emphasis on safety. Furthermore, countries such as the United States have a system where the central or federal government regulates some aspects of vehicles and vehicle operations while state, regional, provincial, or local authorities regulate other aspects. This results in a checkered legal and regulatory environment.[3]

[3] *AI Laws Are Coming*, Forbes, February 20, 2020, https://www.forbes.com/sites/cognitiveworld/2020/02/20/ai-laws-are-coming/#4b886dd1a2b4

3. Analysis of Key National Legislation

3.1 Overview of Key National Legislation

Through EU cybersecurity legislation, implementation frameworks and other related measures, EU cybersecurity and 5G-related strategies have been gradually refined and improved, and they have shown more distinctive regional characteristics, such as attaching great importance to personal data and privacy protection, and paying more attention to cybersecurity cooperation. With the COVID-19 pandemic, globalization has entered a stage of extensive adjustment. The uncertainties facing the 5G global supply chain have increased, and 5G will continue to be the focus of the game between major powers.

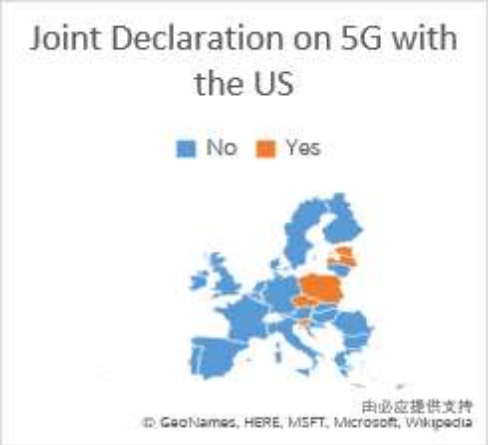

Figure 5: Joint Declaration on 5G with the US[4]

Figure 6: Use Vendors Other Than Huawei

As shown in Figure 5, five EU member states have signed joint declarations on 5G with the US. Poland was the first to do so, followed by Estonia, Latvia, the Czech Republic, and Slovenia, each of which added the word "security" to the declaration title. This reflects a trend of securitization in 5G-related issues. Following the securitization of 5G networks, the government can use security as a basis for taking special measures to intervene in market behavior, such as imposing non-technical standards on suppliers' market access.

[4] Data source: *Europe can't afford to fully ban Huawei*, China Daily, http://epaper.chinadaily.com.cn/a/202007/08/WS5f0511aca3107831ec753538.html.
The Clean Network, United States Department of State, https://www.state.gov/the-clean-network/.
U.S.-Poland Joint Declaration on 5G, The White House, https://www.whitehouse.gov/briefings-statements/u-s-poland-joint-declaration-5g/.
Joint Statement on United States - Czech Republic Joint Declaration on 5G Security, United States Department of State, https://www.state.gov/joint-statement-on-united-states-czech-republic-joint-declaration-on-5g-security/.
Joint Statement on United States - Slovenia Joint Declaration on 5G Security, United States Department of State, https://www.state.gov/joint-statement-on-united-states-slovenia-joint-declaration-on-5g-security/.
United States–Estonia Joint Declaration on 5G Security, The White House, https://www.whitehouse.gov/briefings-statements/united-states-estonia-joint-declaration-5g-security/.

	US-Poland[5]	US-Estonia[6]	US-Latvia[7]	US-Czech[8]	US-Slovenia[9]
Time	2019/09/05	2019/11/01	2020/02/27	2020/05/06	2020/08/13
Principle	• Strengthening cooperation on 5G; • Protecting next generation communications networks from disruption or manipulation; • Ensuring privacy and individual liberties				
Proposals endorsed	Prague Proposals: The Chair's statement at the Prague 5G Security Conference [10]	Prague Proposals: The Chair's statement at the Prague 5G Security Conference	Conclusions on the significance of 5G to the European Economy and the need to mitigate 5G-related security risks[11]; Prague Proposals	Conclusions on the significance of 5G to the European Economy and the need to mitigate5G-related security risks; Secure 5G deployment in the EU – Implementing the EU toolbox[12]; Prague Proposals	Conclusions on the significance of 5G to the European Economy and the need to mitigate 5G-related security risks; Secure 5G deployment in the EU – Implementing the EU toolbox; Prague Proposals; London Declaration[13]
Supplier	Ensure that only trusted and		Encouraging the participation of reliable and		

[5] *U.S. – Poland Joint Declaration on 5G,* The White house, September 5, 2019, https://www.whitehouse.gov/briefings-statements/u-s-poland-joint-declaration-5g/.

[6] *United States – Estonia Joint Declaration on 5G Security*, The White house, November 1, 2019, https://www.whitehouse.gov/briefings-statements/united-states-estonia-joint-declaration-5g-security/.

[7] *Joint Statement on United States – Latvia Joint Declaration on 5G Security*, February 27, 2020, https://www.state.gov/joint-statement-on-united-states-latvia-joint-declaration-on-5g-security/.

[8] *Joint Statement on United States – Czech Republic Joint Declaration on 5G Security,* U.S. Department of State, May 6, 2020, https://www.state.gov/joint-statement-on-united-states-czech-republic-joint-declaration-on-5g-security/.

[9] *Joint Statement on United States – Slovenia Joint Declaration on 5G Security,* U.S. Department of State, August 13, 2020, https://www.state.gov/joint-statement-on-united-states-slovenia-joint-declaration-on-5g-security/.

[10] *The Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitalized world*, Prague 5G Security Conference, https://www.mzv.cz/file/3482865/The_Prague_Proposals.pdf.

[11] *Significance and security risks of 5G technology – Council adopts conclusions*, European Council, https://www.consilium.europa.eu/en/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/.

[12] *Secure 5G deployment in the EU - Implementing the EU toolbox*, European Commission, https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission.

[13] *London Declaration*, NATO, https://www.nato.int/cps/en/natohq/official_texts_171584.htm.

	reliable suppliers participate in our networks		trustworthy network hardware and software suppliers in 5G markets		
Evaluation of Suppliers	Whether the supplier is subject, without independent judicial review, to control by a foreign government; Whether the supplier has a transparent ownership structure; Whether the supplier has a record of ethical corporate behavior and is subject to a legal regime that enforces transparent corporate practices.	Suppliers should not be subject to control by a foreign government without independent judicial review; Financing should be transparent, commercially-based, and follow standard best practices in procurement, investment, and contracting; Ownership, partnerships, and corporate governance structures should be transparent; Suppliers must show commitment to innovation and respect intellectual property rights; Suppliers must have a good track record in terms of respecting the rule of law; the security	Whether the network hardware and software suppliers are subject, without independent judicial review, to control by a foreign government; Whether the network hardware and software suppliers have transparent ownership, partnerships, and corporate governance structures; and Whether the network hardware and software suppliers have a record of ethical corporate behavior and are subject to a legal regime that enforces transparent corporate practices.	Whether the network hardware and software suppliers are subject, without independent judicial review, to undue foreign influence; Whether the network hardware and software suppliers have transparent ownership, partnerships, and corporate governance structures; Whether the network hardware and software suppliers are committed to innovation and respect intellectual property rights; and Whether the network hardware and software suppliers have a record of ethical corporate behavior and are subject to a legal regime	Whether the network hardware and software suppliers are subject, without independent judicial review, to control by a foreign government; Whether the network hardware and software suppliers have transparent ownership, partnerships, and corporate governance structures and are subject to a legal regime that enforces transparent corporate practices; Whether the network hardware and software suppliers are committed to innovation and respect intellectual property rights; and Whether the network hardware and

		environment; suppliers must respect vendor ethics; and suppliers must comply with secure standards and industry best practices to promote a vibrant and robust supply of products and services.		that enforces transparent corporate practices.	software suppliers have a record of ethical corporate behavior.

Table 3: List of EU Member States' Joint Declaration on 5G with the US

It is worth noting that all five joint declarations mentioned above endorsed the Prague Proposals. On May 3, 2019, representatives from 32 countries, including 21 EU member states, and representatives of international organizations such as NATO participated in the 5G security conference in Prague. The Prague Proposals, suggested by the Chairman, were released after this conference and covered four distinct categories: Policy; technology; economy; and security, privacy, and resilience. Within the policy category, it is written that "the overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its governance model, the absence of cooperation agreements on security or similar arrangements such as adequacy decisions regarding data protection, and whether this country is party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection."[14] From this point of view, the risk assessment of 5G suppliers has reached a political level, and even the governance model of the supplier's country of origin has been taken into consideration. Although the Prague Proposals are non-binding, the US government endorsed them through joint declarations on 5G, which further politicalized 5G networks.

In addition, the five joint declarations all mentioned the need for "trustworthy and reliable suppliers to participate in the construction of 5G networks". However, the criteria for judging "trustworthy" and "reliable" are too subjective, allowing governments to label certain suppliers as "untrustworthy", and exclude them from competition. In contrast to the joint declaration on 5G with the US in 2019, the joint declarations on 5G security that were signed by the US with Latvia, the Czech Republic, and Slovenia in 2020, all specified the term "supplier" as "network hardware and software supplier". Considering this, apart from excluding specific suppliers from the infrastructure construction of 5G network hardware, the joint declarations also demanded the exclusion of software provided by so-called "unreliable suppliers". This aligned with the "Clean Store" and "Clean Apps" as part of the Clean Network program launched by the US in June 2020.

Poland, Estonia, Latvia, the Czech Republic, and Slovenia may follow the US's lead and

[14] *The Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitalized world*, Prague 5G Security Conference, https://www.mzv.cz/file/3482865/The_Prague_Proposals.pdf.

introduce similar discriminatory measures to exclude certain network hardware and software suppliers. Their close cooperation with the US makes it even more difficult for the EU to present a united and coordinated front on 5G network construction.

Lessons should be learned from the Nord Stream 2 gas pipeline project. On August 12, 2020, during a videoconference organized by the Delegation of the European Union to the US, 24 EU member states protested US sanctions against the Nord Stream 2 gas pipeline, criticizing that "the extraterritorial application of sanctions by the US is illegal under international law".[15] Notably, three EU member states, including Poland, did not join in this protest. This clearly displays the influence exerted by the US on Eastern European countries, which hinders coordination of foreign policy among EU member states. This, in turn, poses a potential threat to the coherence and unity of EU policies.

In the future, the EU may face the same problem of incoherence when formulating 5G network standards and the related regulations. For instance, the five Eastern European countries may closely follow the American 5G standards-setting and regulatory framework. Whereas the Western European countries, such as Germany and France, are more inclined to form independent and coherent European 5G standards as well as regulatory frameworks.

3.1.1 Germany

(1) Cybersecurity-Related Legislation

As a major power in both industry and information technology, Germany has always attached great importance to ensuring network security. The "Federal Law Regulating the Framework Conditions for Information and Communications Services" ("Multimedia Law") came into effect on August 1, 1997. This Law has made modifications to the Penal Code, the Law on the Distribution of Writings Harmful to Young Persons, the Act on Copyright and the Price Indication Act, based on the needs of the development of information and communication services. In addition, the German government has issued the Telecommunications Data Protection Ordinance. The German government first launched the "Cyber Security Strategy for Germany" in 2011, which includes: The protection of critical information infrastructure and IT systems; improved resistance to cyberattacks; and the promotion of economic and social prosperity by integrating domestic resources and enhancing international cooperation. In July 2015, the Bundestag (German federal parliament) passed the German IT Security Act which set minimum cybersecurity standards and clarified the responsibilities of critical infrastructure operators. Operators of critical infrastructure must report cybersecurity incidents to the German Federal Office for Information Security (BSI), and provide an overview of audits at least every two years to prove they fulfill the security requirements.

1) Telecommunications Act (TKG)

i. Telecommunications Act (1996)

The German Telecommunications Act (TKG), which is composed of 13 chapters and 100 articles, was first promulgated in 1996. The General Provisions of this TKG explains that the purpose of the Act is, through regulation of the telecommunication sector, to promote competition, guarantee appropriate and adequate services throughout the country, and provide for frequency regulation. The aims of regulation shall be to: (1) safeguard the interests

[15] America Hernandez, *EU countries protest US sanctions in warning to Washington*, Politico, August 14, 2020, https://www.politico.eu/article/eu-countries-protest-us-sanctions-say-german-officials/.

of users in the fields of telecommunications and radio communications as well as to maintain telecommunications secrecy; (2) ensure equal-opportunity and workable competition, in both rural and urban areas, in telecommunications markets; (3) ensure the provision of basic telecommunications services (universal services) throughout the Federal Republic of Germany at affordable prices; (4) promote telecommunications services in public institutions; (5) ensure effective, interference-free use of frequencies, with due regard also being paid to broadcasting requirements; (6) protect public safety interests[16].

ii. Telecommunications Act (2004)

On June 22, 2004, Germany released a new version of the Telecommunication Act, which exceeded 100 sections (a total of 152) for the first time. Section 109 consisted of technical safeguards to protect network security. Section 109 (1), (2), (4), (6) are listed as follows:

Section 109 (1): Every service provider must take necessary technical precautions and other relevant measures to:

a. protect the secrecy of telecommunications.

b. ensure the protection of personal data.

The state of the art must be taken into account.

Section 109 (2): Anyone who operates a public telecommunications network or provides publicly accessible telecommunications services must take the appropriate technical precautions and other related measures for all telecommunications and data processing systems operated for this purpose to:

a. protect against disruptions that could lead to the considerable impairment of telecommunication networks or services, including those that could be caused by external attacks or disasters.

b. control risks to the security of telecommunications networks and services.

Section 109 (4): Anyone who operates a public telecommunications network or provides publicly accessible telecommunications services must appoint a security officer and create a security concept that shows:

a. which public telecommunications network is operated and which publicly accessible telecommunications services are provided

b. what hazards are to be assumed

c. which technical precautions or other protective measures have been taken or planned to fulfill the obligations under Section 109 (1) and (2).

Any entity that operates a public telecommunications network must submit its security concept to the Federal Network Agency (BNetzA) immediately after the network starts operating. Any entity who provides publicly accessible telecommunications services can be obliged by the Federal Network Agency to submit its security concept after it starts providing telecommunications services. A declaration must be submitted, along with the security concept, stating that the technical precautions and other protective measures shown therein

[16] Telecommunications Act of 25 July 1996, International Telecommunication Union, https://www.itu.int/ITU-D/treg/Legislation/Germany/TelecomAct.pdf.

Overview of the German Telecommunications Industry, Economic and Commercial Section of the Embassy of the People's Republic of China in the Federal Republic of Germany, September 15, 2005, http://de.mofcom.gov.cn/article/ztdy/200510/20051000500920.shtml.

have been implemented or will be implemented immediately. Where the Federal Network Agency establishes insufficient security in the security concept or during its implementation, it may require the operator to eliminate such shortcomings. If the conditions upon which the security concept is based change, the party that is obliged must adapt the concept and resubmit it to the Federal Network Agency, referencing the changes. The Federal Network Agency regularly reviews the implementation of the security concept. The review should take place at least every two years.

Section 109 (6): In agreement with the Federal Office for Information Security and the Federal Commissioner for Data Protection and Freedom of Information, the Federal Network Agency created a catalogue of security requirements for the operation of telecommunications and data processing systems, the processing of personal data as a basis for the security concept according to Section 109 (4), and technical precautions and other measures to be taken according to Section 109 (1) and (2). This catalogue gives manufacturers, associations of operators of public telecommunications networks, and associations of providers of publicly accessible telecommunications services the opportunity to provide their comments and suggestions. The catalogue is published by the Federal Network Agency.

(2) Catalogue of Security Requirements

In view of the large-scale deployment of 5G and the latest situation surrounding international security, the German Federal Network Agency issued a draft of the new catalogue of security requirements on March 7, 2019. According to Section 109(6) TKG, this catalogue should be drawn up by the Federal Network Agency, in agreement with the Federal Office for Information Security (BSI) and the Federal Commissioner for Data Protection and Freedom of Information (BfDI). The updated catalogue of security requirements (version 2.0) was released on October 9, 2019. Its contents were adjusted accordingly, such as adding certification requirements for critical infrastructure components, specific regulatory compliance requirements, and supplier share requirements. On August 11, 2020, the Federal Office for Information Security issued a draft of the Catalogue of Security Requirements for Operating Telecommunications and Data Processing Systems and for Processing Personal Data (version 2.0), and the List of Critical Functions for Public Telecommunications Networks and Services with a High Level of Risk. Responses to the list of critical functions must be submitted by September 30, 2020.

The updated catalogue of security requirements[17] added the following:

- Abnormal network traffic must be monitored on a regular and continuous basis. If there are any doubts regarding network traffic, appropriate protective measures should be taken, such as stopping network traffic completely, limiting or stopping traffic from interfering sources, etc. Testing must consider the latest technology.
- Security-related network and system components (critical core components) can only be used after a successful IT security inspection by a testing organization that is approved by the Federal Information Security Agency and after receiving a BSI certification. Critical core components can only be purchased from suppliers and manufacturers that can guarantee their trustworthiness through appropriate means. This obligation applies across the entire supply chain and is a requirement for the necessary certification of components.
- Security-related network and system components (critical core components) will

[17] *Telecommunications Security*, Bundesnetzagentur, https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/ServicerProviderObligation/TelecommunicationSecurity/TelecommunicationSecuritynode.html.

be jointly determined by the Federal Information Security Agency and the Federal Network Agency when compiling the catalog.

- Security-related network and system components (critical core components) can only be used after the appropriate acceptance tests during the delivery period and regular security tests. Any discrepancies with the service specifications of a network operator or provider identified during testing must be recorded, and appropriate risk measures must be taken. The Federal Network Agency and the Federal Information Security Agency must be immediately notified of any measures taken to minimize the risk of deviations that could significantly impact telecommunications networks or services.
- Evidence must be provided to prove that the hardware for testing the safety-related components within a selected product and testing the source code at the end of the supply chain have been deployed.
- When planning and constructing a network, networks and system components from different manufacturers must be used to ensure sufficient diversity. This requirement will be further defined by the Federal Network Agency, and differences may exist between different networks, such as between core networks and access networks.
- When outsourcing system-related processes, network operators and providers must use independent, professional, and reliable contractors and ensure compliance with legal requirements. Network operators and providers must provide proof of this.
- Sufficient redundancy must be provided for key network and system components (critical core components) that are related to security. In this regard, a list of particularly critical network components is being developed, including home location registers, core networks, backbone networks, and port servers.
- All security requirements must match national security regulations related to telecommunication confidentiality and data privacy protection.

The List of Critical Functions for Public Telecommunications Networks and Services with a High Level of Risk is as follows:

Category	**Functionalities**
1. Subscriber management and cryptographic mechanisms (if a network component)	-Session management functions -Key management for subscribers and network components -Functions for secure authentication, integrity protection and key storage for subscribers, network components and management components. -Access policy management
2. Cross network interfaces	-Roaming functions (signaling, CDR exchange, fraud detection systems), -Telephone number portability and reverse number lookup -Connection to third party provider networks

3. Managed network services	-Registration and authorization of network services -Storage of subscriber and network data -Exposure of network functions to external applications
4. NFV Management and Network Orchestration (MANO), as well as virtualization	-Management functions for orchestration and configuration of NFV -Virtualization functions for implementing NFV
5. Management systems and other support systems	-Functions of the management system -Installation and administration of virtual subnetworks -Network performance
6. Transport and information-flow control	-Highly important voice and data transport functions
7. Lawful interception	-Access to content and subscribers' metadata by authorized bodies

Table 4: List of the Critical Functions[18]

Germany takes a pragmatic approach in terms of improving cybersecurity and has placed more emphasis on technology audits for the relevant cybersecurity legislation. Notably, the new catalogue of security requirements adds a new requirement for the procurement of critical core components that, in addition to a Federal Information Security Agency certification, can only be procured from trustworthy suppliers and manufacturers. Nevertheless, it remains unclear how to define component reliability and what the evaluation criteria are. As required by the EU, the German government has until the end of 2020 to finish revising the Telecommunications Act, and German telecom companies are still waiting for the government to publish the details regarding security standards.[19]

(3) US Influence on Germany

Despite lobbying and pressure from the US, the German government still insists on maintaining objective cybersecurity standards that align with its national interests. In March 2019, the US Ambassador to Germany Richard Grenell wrote to German Economy Minister Peter Altmaier. In this letter, he warned that the US would restrict intelligence and other information sharing with Germany if Huawei or other Chinese suppliers were allowed to participate in Germany's 5G network construction. Facing US pressure, German Chancellor Angela Merkel highlighted the importance of national sovereignty when defining "security

[18] *List of the critical functions for public telecommunications networks and services with a high level of risk*, Bundesnetzagentur, https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/Telecommunication%20security/criticalFunctionsTK_pdf.pdf.

[19] *The German Federal Government intends to encourage network operators to strengthen cooperation*, Ministry of Commerce of the People's Republic of China, August 10, 2020, http://www.mofcom.gov.cn/article/i/jyjl/m/202008/20200802992097.shtml.

standards". "Security, particularly when it comes to the expansion of the 5G network, but also elsewhere in the digital area, is a very important concern for the German government, so we are defining our standards for ourselves." she said[20]. In November 2019, US Secretary of State Mike Pompeo asked Germany to exclude Chinese companies from 5G network construction on the grounds of cybersecurity concerns. In response, German Chancellor Angela Merkel said that Germany attaches great importance to the security requirements and verifiability of enterprises involved in 5G network construction. However, it will not set standards for specific suppliers.

3.1.2 France

(1) The Act on 5G Network Security

On July 3rd, 2019, the French joint committee (CMP) passed the Act on 5G Network Security to legislate on mobile wireless network operations in the interest of national defense and national security. The law is aimed at establishing a new authorization system for 5G equipment to be used in France to protect network information security and national science and technology capacity. The bill was passed by the French National Assembly (the Lower House) on April 10th and by the French Senate (the Upper House) on June 27th.

The law which went into effect in September, 2019 mandated the establishment of a business approval system wherein operators must first obtain authorization from the French government before they can operate mobile wireless network equipment (primarily 5G equipment) that may affect the integrity and security of French networks. This authorization must be issued by the Prime Minister and will remain valid for a maximum of 8 years. The term "mobile wireless network equipment" as mentioned in the Act refers to any device that can connect the user's mobile phone, computer, or other terminal devices to a mobile network.

The prime minister is required to investigate these operators' equipment deployment contracts and whether any of the involved operators and equipment suppliers under the control or influence of governments outside the European Union. The Prime Minister may refuse to issue an authorization if they consider any involved equipment a threat to national security.

The act also mandates the creation of a list of specific punishments for illegal actions related to this act. A grace period must be set for operators and suppliers who failed to obtain an authorization from the government before they begin operations, during which time they can submit a supplementary authorization application. If no such application is submitted, the related operation contracts will be deemed invalid. Unauthorized network operation should result in prison sentences of up to five years and fines up to 300,000 euros.

(2) Different License Terms for Different Telecom Operators

In early July, French authorities told telecom operators planning to buy Huawei 5G equipment that they would not be able to renew their equipment licenses. This effectively pushed operators to phase Huawei equipment out of their mobile networks because of their varying license periods.

The French National Cybersecurity Agency ("ANSSI") stated on July 6th that operators will be allowed to use equipment from Huawei, but urged telecoms companies to not change their

[20] Andrea Shalal, *Germany assets independence after US warning on Huawei*, Reuters, March 12, 2019, https://www.reuters.com/article/us-germany-huawei-merkel/germany-asserts-independence-after-us-warning-on-huawei-idUSKBN1QT1PV.

equipment from other suppliers to Huawei's. The current licenses of these operators were set to expire in three to eight years. Each operator had to apply for dozens of equipment licenses to cover different parts of the country but there were reports that ANSSI had already informed operators of its licensing decisions for big cities. Most Huawei equipment was supposedly licensed for three to five years, compared with the eight year licenses that were issued for its European rivals, Ericsson and Nokia. Neither the ANSSI nor the companies involved have publically announced these results though.

The head of ANSSI Guillaume Poupard said this move was aimed at protecting French independence, because the risks presented by all non-European suppliers are different than those presented by European suppliers, so was not a move specifically directed at China or Huawei. However, some believe this will make telecom operators specifically unwilling to invest in Huawei equipment, as new mobile technologies such as 5G will take at least eight years to reach a return on investment. "A three-year period is equivalent to a ban".

(3) Act R226

The French government introduced R226 to the penal code in 2010. According to the latest amendments to R226, all communications equipment manufactured, imported, exhibited, supplied, leased and sold in France, including lawful interception devices, requires authorization from the French Government. Operators also need to obtain R226 authorization to import, purchase, and use these devices. These communications devices also need to be re-certified when they undergo large-scale software updates or hardware platform updates.

At present, this work is mainly carried out by an advisory committee headed by the Prime Minister, and chaired by the ANSSI director or their representative. R226 stipulates that the Prime Minister is responsible for issuing a list of specific instruments and technical equipment requiring certification authorization, and the ANSSI director is responsible for reviewing authorization applications. The Committee also includes representatives from the judiciary; the departments of the interior, defense, and telecommunications; national industry; state intelligence; and other sectors. The Committee is empowered to make, amend, and issue orders under R226, related to the authorization of manufacturing and sales under R226.[21]

R226 will be a potential barrier for telecommunication companies to enter the French market, including those from China. If telecommunications equipment does not receive both R226 authorization and renewal authorization, local operators will be unable to use it. The R226 authorization process is relatively strict and long, taking several months to complete, which will seriously hinder the entry of foreign suppliers, such as Huawei, to the French market. It is worth noting that while R226 authorization is important for entering the French market, there are no strict authorization standards defined for the commission to use. This means authorization can be easily influenced by France's national policy and diplomatic orientation.

(4) The US Factor in 5G Cybersecurity Policy

France recently issued an informal notice telling telecom network operators that licenses for 5G equipment purchased from Huawei would not be renewed after they expire. At present, licenses for Huawei equipment are generally valid for 3-5 years, far less than the 8-year licenses issued for equipment from Ericsson or Nokia. This move will likely affect Huawei's subsequent license applications and increase procurement resistance from local operators. It also means that France could choose to remove Huawei equipment by 2028, similar to Britain's order to remove Huawei equipment by 2027, which would essentially cover the operational

[21] *Criminal Code of the French Republic*, Legislationline, January 2020, https://www.legislationline.org/download/id/8546/file/France_CC_am012020_fr.pdf

cycle of 5G technology.[22]

The US has consistently pressured France on 5G network security, and its policy orientation has fluctuated and changed accordingly. On November 25, 2019, a junior economic minister said France would not follow the US in excluding Huawei from its next generation of 5G development, but will reserve the right to review all equipment manufacturers for potential security threats.[23] On July 21, 2019, French Finance Minister Jean-Pierre Lemaire said France would not ban Huawei from investing in the construction of non-sensitive 5G networks[24]. Multiple statements made by the French government indicated that they felt including Huawei domestic 5G network construction would be beneficial to national development, despite the fact it ran counter to the US's policy of exclusion. Both Britain and France were put under constant pressure to reconsider from the US though. On July 22, 2020, the ANSSI said that telecom operators with legitimate 5G business licenses will be allowed to purchase Huawei 5G equipment and government officials made it clear that Huawei would not be banned from investing in 5G in France.

France's strategic direction indicates that their relationship with the US will further solidify, which means pressure from the US will have an increasing impact on France. France did not make firm determination on 5G network construction though and responded with fluctuating and vague attitudes and statements. France has anti-Americanism tradition and Gaullists have one of the most powerful voices in France. Macron also advocated anti-American stances when he came to power to pursue a Gaullist approach to safeguarding France's national interests and global influence. Although France currently stands in line with the US, it wants to avoid tipping the scales to any one major power. It also wants to increase its influence and leadership in European affairs. As Chinese 5G technology offerings are comprehensive, cost effective, value added and secure, France currently views them favorably. Therefore, in terms of the overall strategic choice, France will almost definitely continue to side with the US in the long-term to safeguard its overall national interests. But when it comes to specific issues, especially for the choice of emerging future technologies such as 5G, France may still act independently.

3.1.3 Italy

(1) National Cybersecurity Strategy

The Italian government issued three national strategies related to cybersecurity in 2013, 2015 and 2017, respectively. In December 2013, the Italian government launched the National Strategic Framework for Cyberspace Security that highlighted the nature and the evolving trends of cyber threats, as well as of the vulnerabilities found in national ICT networks. Four types of threat were identified which includes cybercrime, cyber espionage, cyber terrorism, and cyber warfare. The roles and responsibilities of public and private stakeholders were outlined in this strategy. The framework also identified tools and procedures to enhance the country's preparedness to confront the new challenges posed by cyberspace head-on. The

[22] *Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028*, Reuters, July 22, 2020, https://www.reuters.com/article/us-france-huawei-5g-security-exclusive/exclusive-french-limits-on-huawei-5g-equipment-amount-to-de-facto-ban-by-2028-idUSKCN24N26R

[23] *France will not exclude China's Huawei from 5G rollout: minister*, Reuters, November 25, 2019, https://www.reuters.com/article/us-france-huawei-minister/france-will-not-exclude-chinas-huawei-from-5g-rollout-minister-idUSKBN1XZ1U9

[24] *Huawei will not be prevented from investing in France, says French finance minister*, The Economic Times, July 21, 2020, https://economictimes.indiatimes.com/news/international/business/huawei-will-not-be-prevented-from-investing-in-france-says-french-finance-minister/articleshow/77081572.cms

National Plan, which was attached to this strategy, identified a limited set of priorities, and provided specific objectives as well as guidelines on the implementation of this framework[25].

In 2015, the Italian Minister of Defense signed a White Paper on International Security and Defense which identified cyber as a domain to be addressed and defended, and linked cybercrimes with cyber war. According to the white paper, civil authorities should have jurisdiction over cybercrime and the Ministry of Defense over cyber war. This white paper recognized not only the urgent need for a legal definition of cyber space, but also the danger of competition between political and military leadership over issues related to hybrid warfare. Moreover, it called for coordination between civil and military security strategies.

On May 31, 2017, the Italian government launched the National Plan for Cyberspace Protection and ICT Security which established another framework for cybersecurity and data protection. This national plan covered four main points: (1) extending the framework laid out in the 2013 National Strategy and Plan; (2) strengthening intelligence gathering and public-private cooperation; (3) shortening cybersecurity chain of command and increasing the authority of the director of the Department of Information Security; and (4) outlining a process to establish a national ICT assessment center, a national cybersecurity research center, and a national encryption center.

(2) Relevant Laws, Regulations and Legislative Trends

1) Decree-Law No. 64/2019

On July 11, 2019, Italy adopted Decree-Law No. 64/2019 ("DL 64/2019") to expand the Italian government's power to set and veto criteria for the transactions on 5G broadband telecommunications services. DL 64/2019 also mandated that the government be notified before any important strategic activities related to national defense and national security. As early as 2012, two legal amendments, Decree-Law No. 21/2012 and Decree-Law No. 56/2012, gave the state the right to interfere in the transactions of companies involved in "strategic sectors" such as defense, national security, communications, energy, and transportation. This power of intervention is called the "golden power", because the Italian government can use administrative power to invalidate signed contracts without incurring fines.

DL 64/2019 modified that "golden power to strengthen national security in strategic sectors while also expanding the definition of strategic sectors to include new areas related to 5G technologies. In addition, the decree-law also strengthened the government's investigative powers and significantly extended the time frame in which government could exercise its "golden powers" in all strategic sectors. The timeframe for investigation was extended from 15 days to 45 days, giving the government an additional month to investigate transactions. The government was also given explicit authority to conduct specific examinations of any third party, such as a public or regulatory body or a company's managers, shareholders, and auditors to obtain relevant information. If the Italian government requests information on any future transactions, both involved parties are required to provide the requested information within 30 days of receipt of the request rather than within 10 days. Nevertheless, while the extended investigation period gives the Italian government significantly more time to assess risks to national security, it also increases the possibility of delaying those commercial deals.

In addition, in the communications, energy, and transportation sectors, DL 64/2019 further defined the term "non-EU purchaser" in mergers and acquisitions transactions to identify transfers of strategic assets to non-EU entities. This new definition includes not only legal entities explicitly established outside EU territories, but also some entities formally established in an EU Member State and controlled entities whose principal place of business

[25] *Italy: Cybersecurity Policy*, UNIDIR Cyber Policy Portal, April, 2020, https://unidir.org/cpp/en/states/italy.

is in the EU. Entities operated directly or indirectly by non-EU individuals or companies are also included.

2) Decree-Law No. 105/2019

On September 21, 2019, the Italian Council of Ministers adopted Decree-Law No. 105/2019 ("DL 105/2019") to create a "national cybersecurity perimeter". This decree-law named 5G-based broadband telecommunications services as strategic activities. This authorized the Italian government to exercise its "golden powers" over 5G technology contracts, and allows it to veto company decisions on related businesses. Article 3 of DL 105/2019 includes provisions related to 5G-powered broadband networks. Paragraph 2 specifically identified the following types of 5G transactions: (i) Procurement of goods and services that are related to the design, construction, maintenance, and operation of 5G-powered broadband service networks, and (ii) acquisitions of high intensity technology that will be implemented with entities outside the EU.[26] Failure to notify the appropriate bodies of such transactions or to comply the relevant regulations will result in severe sanctions against the entities involved. The Italian government has the power to order an interpretation of the relevant transactions and restore the previous status quo at the expense of the parties involved.[27]

DL 105/2019 also provided that the act must be converted into a fully enforceable law by parliament within 60 days of its promulgation, otherwise, it would lose its effectiveness. Within 60 days, on November 18, 2019, urgent provisions on national cybersecurity to this effect were passed by the Italian parliament through Law No. 133/2019. The law also imposed new rules and obligations on private groups that provide strategic services at the national level. Such groups are now required to ensure a high level of security in IT systems and networks, and could be fined up to 1.8 million euros for breaches. Based on a previous amendment made by the Senate, this law also included a rule which assigned to the Interior Ministry its own accredited assessment center for ICT networks and supplies of competence[28].

This cybersecurity legislation defined the scope of Italy's national cybersecurity to ensure a high degree of security in networks, information systems, and IT services. Parties whose operations would fall within the scope of national cybersecurity include: (i) parties involved in activities, such as malfunction, interruption, or improper use of the aforementioned networks, information systems and IT services; and (ii) parties that exercise an essential function of the State, or ensure an essential service for the maintenance of civil, social or economic activities essential for the interests of the State. The President of the Council of Ministers then required that parties under the jurisdiction of national cybersecurity legislation had to be defined by March 21, 2020. Public administrations, public and private entities, and operators with a registered office in Italy, are required to comply with the measures and obligations set out in this legislation. These parties were then given six months to submit a list of their network information systems, and IT services to the Office of the President of the Council of Ministers and the Ministry of Economic Development. The list is updated at least once a year.

---

[26] *Italy moves on cybersecurity*, Simmons-Simmons, October 18, 2019, https://www.simmons-simmons.com/en/publications/ck20awkn8cwfy0b19pj0vejpx/italy-moves-on-cybersecurity.

[27] Leah Dunlop, Elisabetta Randazzo, Niccolò Lavorano and Anastasia Pallagrosi. *Italy: Italian Government Acts To Strengthen Further Its "Golden Powers"*, Hogan Lovells, August 09, 2019, https://www.mondaq.com/italy/terrorism-homeland-security-defence/830534/italian-government-acts-to-strengthen-further-its-golden-powers.

[28] *Il decreto sulla cybersicurezza è legge. Alla Camera il voto dell'ok definitivo*, La Repubblica, 13 novembre, 2019, https://www.repubblica.it/politica/2019/11/13/news/cybersicurezza_legge-241041589/.

Italy expands to the 5G field through the "Golden Power" of the Cybersecurity Law, Economic and Commercial Section of the Embassy of the Ministry of Commerce of the People's Republic of China in the Republic of Italy, November 13, 2019, http://it.mofcom.gov.cn/article/jmxw/201911/20191102914026.shtml.

This cybersecurity legislation aimed to strengthen Italian government's control over network construction and national cybersecurity. It did not target specific telecom equipment suppliers such as Huawei. However, the expansion of the government's "golden powers" has created some obstacles for Huawei's participation in Italian 5G network construction.

To sum up, within two months, Italy successively passed DL 64/2019 and DL 105/2019, which authorized the Italian government to directly intervene in the telecommunication industry as it is a strategic sector. The cybersecurity legislation passed in November 2019 codified the "golden powers" of the Italian government into law, and determined that the government's use of administrative powers could be extended to the commercial construction of 5G networks. This "golden power" was continuously strengthened both horizontally and vertically by widening both its scope and the power. The Italian government can therefore use the "golden power" to intervene in telecommunications industry transactions, including those related to commercial 5G services. This will not only distort market competition, but also delay the purchase and deployment of 5G facilities. This will increase uncertainty between telecom operators and 5G equipment suppliers.

3) Simplification Decree-Law No. 76/2020

In July 2020, Decree-Law No. 76/2020 ("DL 76/2020") on "urgent measures for simplification and digital innovation" was released. According to Article 38 of the decree, the mayors of individual municipalities would, "not be able to introduce restrictions on the localization of radio base stations for any type of electronic telecommunications networks on their territory and shall not set limits for exposure to electric, magnetic and electromagnetic fields other than those established by the State."[29] The DL 76/2020 blocked all local decrees opposing the installation of 5G antennas. Ernst & Young Consulting predicts 17% of Italians are expected to be using 5G by the end of 2020, and 31% by the end of 2021. This will make Italy one of the major 5G markets in Europe.

(3) 5G Commercial Deployment in Italy

Frequency band	**Spectrum assigned**	**Available starting**	**Channel width**	**Coverage obligations**	**License duration (years)**
700MHZ	Not Specified	July 2020	5 MHz duplex	Required	15.5
3.4-3.8GHZ	200MHz (3.6-3.8GHz)	Yes	20 MHz	Required	19
26GHZ	1GHz (26.5-27.5GHz)	Yes	200 MHz	No	19

Table 5: Italy's 5G Strategy (from technical aspect)[30]

[29] *5G: i sindaci non potranno introdurre limitazioni*, ANSA, 23 July, 2020, https://www.ansa.it/sito/notizie/tecnologia/tlc/2020/07/22/5g-sindaci-non-potranno-introdurre-limitazioni_e93998bb-4a2b-4943-8e60-637e847e1edb.html.

[30] *Data source: 5G Observatory Quarterly Repo*rt (Up to June 2020), IDATE DigiWorld, July, 2020 http://5gobservatory.eu/wp-content/uploads/2020/07/90013-5G-Observatory-Quarterly-report-8_1507.pdf.

Figure 7: Italy's 5G Strategy (Deployment Timeline)[31]

Two major Italian telecom operators, Telecom Italia (TIM) and Vodafone Italy, began 5G commercial construction in June 2019, while the third largest telecom operator, Wind Tre, planned to start commercial construction in 2020. According to Reuters, in July 2020, TIM did not invite Huawei to submit a bid for core 5G network construction in Italy and Brazil.[32] Luigi De Vecchis, president of Huawei Italy, said in an interview that TIM's decision to exclude Huawei from suppling 5G equipment was a commercial, rather than a geopolitical.[33] The Italian government has not banned Huawei from supplying 5G equipment, however, the Italian government can legally exercise its "golden power" to review 5G transactions between Italian telecom operators and non-EU suppliers.

(4) The US Influence on Italy

On February 15, 2019, the US ambassador to Italy Lewis Eisenberg met with Deputy Prime Minister Luigi Di Maio in Rome. Ambassador Eisenberg attempted to pressure the government on issues such as opening the 5G market to Huawei and Italy's participation in China's Belt and Road Initiative. He expressed concern over Italy opening up its 5G market to Chinese companies given the presence of several NATO and US agencies in Italy, and the risk that their data could be stolen or monitored by China. The ambassador requested the Italian government be cautious of any cooperation with Chinese telecommunications companies to protect its own national security and that of its allies. The Deputy Prime Minister therefore established a special security department under the Ministry of Economic Development by ministerial decree for national security. This department is responsible for monitoring data and information flows through new networks. The monitoring process will be comprehensive including preventive control and supervision. Moreover, he promised that Italy treasures US recommendations and is preparing to set up a technical and regulatory shield to prevent any data leaks.[34]

---

[31] *Data source: 5G Observatory Quarterly Report* (Up to June 2020), IDATE DigiWorld, July, 2020 http://5gobservatory.eu/wp-content/uploads/2020/07/90013-5G-Observatory-Quarterly-report-8_1507.pdf.

[32] *Exclusive: TIM excludes Huawei from 5G core equipment tender*, Reuters, July 9, 2020, https://www.reuters.com/article/us-huawei-tech-5g-italy-brazil-exclusive/exclusive-tim-excludes-huawei-from-5g-core-equipment-tender-in-italy-brazil-idUSKBN24A2AE.

[33] *Huawei says it's working with Telecom Italia despite 5G exclusion*, Reuters, July 20, 2020, https://www.reuters.com/article/us-huawei-italy/huawei-says-its-working-with-telecom-italia-despite-5g-exclusion-paper-idUSKCN24L0IM.

[34] Marco Galluzzo, *Gli Stati Uniti avvertono l'Italia sui rischi del 5G in mano ai cinesi*, Corriere della Sera, February 18, 2019, https://roma.corriere.it/notizie/politica/19_febbraio_18/gli-stati-uniti-avvertono-l-italia-rischi-5g-mano-cinesi-aaef44b2-33af-11e9-8ba2-1cae66b0283a.shtml.

The United States warns of the risks of Italy and Huawei's 5G cooperation, Ministry of Commerce of the People's Republic of China, February 19, 2019, http://www.mofcom.gov.cn/article/i/jyjl/m/201902/20190202836357.shtml.

On August 16, the US Secretary of State for Economic Growth, Energy, and the Environment Keith Krach gave an interview to La Stampa which was headlined "China is already using TikTok to spy on you. Italy should not hand over its 5G network to Huawei now."[35] Krach urged Italy to join the US Secretary of State Mike Pompeo's Clean Network and 5G Clean Path initiatives, claiming the Clean Network program would prevent "distrusted telecommunications providers", i.e. Chinese companies, from participating in building Europe's next-generation networks.

Italy has not barred Huawei from its 5G network for now, despite this pressure. However, according to a July 8, 2020 Reuters' report, an Italian political source said the government was considering excluding Huawei from building its 5G network construction.[36] The source said that now Foreign Minister Luigi Di Maio has recently met with the US ambassador to discuss issues including Huawei.

3.1.4 Spain

(1) Spain's 5G Legislation Status

Spain's legislation in the field of 5G is relatively comprehensive, based on a systematic 5G deployment strategy that extends from the international level to the regional level.

In 2013, the Spanish government established the PEBA-NGA State Aid scheme to accelerate the deployment and coverage of Next Generation Access (NGA) networks in underserved areas through subsidies to telecommunications operators. The 2014 Spanish Telecoms Law and other industry regulations were then passed to reduce regulatory and administrative barriers and create an investment-friendly environment for ultra-fast networks. At the same time, these regulations solidified technology neutrality in Spain and began related business in various regions through a public-private cooperation mechanism.

At present, Spain's 5G network development is primarily based on two major policy documents:

1. The March 2014 *Digital Agenda for Spain*, which provided strategies for deploying ultra-fast networks and services, and formulated a radio spectrum management plan. According to the agenda, Spain should reach 100% 30 Mbps coverage and 50% 100 Mbps coverage by the end of 2020. In order to achieve this goal, Madrid has formulated 9 specific measures, including effective use of existing social structures to minimize deployment costs; strengthening company cooperation and inter-departmental coordination; launching new spectrum and accelerating 4G network deployment; access mobile broadband networks in areas with small populations with appropriately lower standards; and so on. These measures have laid a good foundation for Spain's current 5G development, and cleared obstacles in terms of infrastructure, management methods, technical standards, and market acceptance.

2. The *5G National Plan 2018-2020* which is based on the *EU's 5G Action Plan*. Implementation of this plan has already begun (as shown in Figure 10). The plan states Spain's 5G development is based on 4 pillars: (1) Radio spectrum management and planning; (2) network and service pilot projects; (3) a regulatory framework for a flexible legal framework;

[35] Keith Krach *La Cina già vi spia con TikTok. Ora l'Italia non dia il 5G a Huawei*, La Stampa, August 16, 2020, https://www.lastampa.it/topnews/primo-piano/2020/08/16/news/keith-krach-la-cina-gia-vi-spia-con-tiktok-ora-l-italia-non-dia-il-5g-a-huawei-1.39198080.

[36] *Italy considering whether to exclude Huawei from 5G: report*, Reuters, July 8, 2020, https://www.reuters.com/article/us-huawei-italy/italy-considering-whether-to-exclude-huawei-from-5g-report-idUSKBN2491C1.

and (4) 5G plan coordination and international cooperation. Currently, Spain has completed the bidding and licensing for the 3.4-3.6 frequency band, and is now developing a 5G pilot project. The government's 5G network supervision work focuses on five major goals: privacy protection, network security, user rights, service quality, and infrastructure.

Figure 8: Spain's 5G National Plan 2018-2020[37]

Spain's 5G legislation is based on EU law. In addition to the national legislation and strategic documents, the autonomous communities of Galicia, Valencia, the Basque Country, Aragón, Andalusia, Catalonia, and Castile and León have also developed their own 5G plans and strategies. As a result, Spain has formed a systematic and effective 5G development model, and at the same time can effectively monitor the implementation within the legal framework. Through the rational use of financial resources, private sector investment, European funds, and other sources of funds, Spain has made a breakthrough in 5G network construction.

Currently, Spain is one of the largest telecommunications markets in Europe, with a population of more than 46 million. The Spanish mobile penetration rate is about equal to the European average, but there is still room for growth. The fiber optic network deployed in Spain is the most extensive in Europe, with more than 33.3 million access points, covering more than 75% of the population. Due to the continuous investment in infrastructure by telecommunication operators, Spain has been developing well in the mobile broadband field. Spain's 4G coverage rate exceeds 95%, and major operators have shifted their focus to 5G services. Vodafone Spain started to develop its 5G network at the end of 2019, and currently provides services primarily in the 3.5 GHz frequency band. The Spanish government decided to postpone the bidding and deployment of the 700 MHz frequency band spectrum due to COVID-19, but this did not significantly impact the overall plan for 5G network construction. Vodafone's CEO also said that it will work with Huawei and Ericsson to deploy its 5G networks.

(2) Spanish 5G Regulatory Agencies

Currently, Spain's national broadband strategy is regulated by two major institutions: the National Commission of Markets and Competition ("CNMC"), and the Secretary of State of Digitization and Artificial Intelligence ("SEAD") under the Ministry of Economic Affairs and Digital Transformation.

The CNMC has undergone a series of significant organizational changes since its founding. Spain had established the National Electric Power System ("CNE") in 1995, the Telecommunications Market Commission ("CMT") in 1996, the Railway Regulatory

[37] *Spain's 5G National Plan 2018-2020*, https://avancedigital.gob.es/5G/Documents/plan_nacional_5G_en.pdf.

Commission ("CRF") in 2003, the State Council's Audiovisual Media Council ("CEMA") in 2010, the National Council of Postal Services ("CNSP") in 1998, the National Competition Commission (CNC) in 2007, and the Airport Economic Management Committee ("CREA") in 2011. In 2013, these institutions were combined to become the CNMC, strengthening the independence of regulatory agencies and competition management agencies and increasing legal security and institutional trust (Figure 9). The committee currently has two governing bodies: the council and the chairman. The council consists of 10 members appointed by the Ministry of Economic Affairs and Digital Transformation. All members are required to be reputable, recognizable, and competence in their field of expertise. The chairman is appointed by the members of the council for a term of 6 years and cannot be re-elected. The chairman is primarily responsible for: (1) the general plan, which is executed by the Ministry of Competition and the Supervision Department, which is responsible for supervision tasks; and (2) specific matters specific matters pertaining to the Ministry of Competition, the Ministry of Telecommunications and Audiovisual, the Ministry of Energy, and the Ministry of Transport and Post, who are in turn responsible for resolving disputes in their corresponding fields.

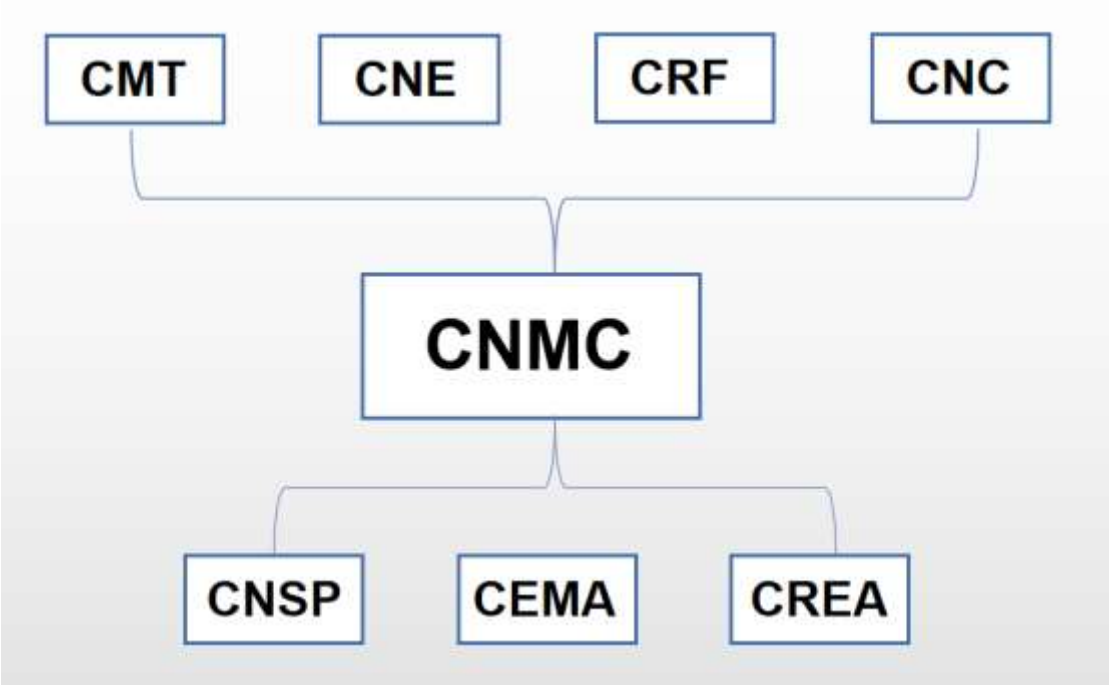

Figure 9: The National Commission of Markets and Competition (CNMC)

The SEAD has two secretaries: the Secretary of State for Digitization and Artificial Intelligence, who is primarily responsible for the General Secretariat for Digital Administration, and the Secretary of State for Telecommunications and Digital Infrastructures, who is mainly responsible for the General Directorate of Telecommunications and Organization of Audiovisual Communication Services. They jointly implement government policies and make recommendations to promote Spain's digital transformation and the development of artificial intelligence. The Secretary of Digitalization has incorporated public policies on the telecommunications and information society, and introduced political policies to strengthen the digital enterprise ecosystem.

In addition, individual provinces in Spain have established Provincial Headquarters of Telecommunications Inspection to solve specific issues in telecommunications services, such as identity authentication, technical direction, rights and obligations, etc.

(3) Spanish 5G Supplier Qualification Review

Spain's management of telecommunications service providers focuses on technological advancement, user rights, and ensuring personal privacy will not be compromised due to technological development. The Information Society and E-Commerce Services Law stipulates that telecommunications service providers are obliged to inform customers of technical tools they have to protect information security (such as anti-virus software, anti-spyware, mail filters, etc.), and at the same time clearly filter and restrict certain content and tools from certain services.

Similarly, Spain's 5G supplier qualification evaluation also considers technical capabilities as its primary criterion, and then considers security issues. Spain requires suppliers have the technical capabilities to adapt to the status quo of Spain's 5G development and meet its future development needs. In other words, Spain basically used technical capabilities as a measurement standard for 5G suppliers, and then imposed further security requirements. Thus suppliers will not be selected based on their country of origin. Based on these technical standards, Spain has had a good relationship with Huawei.

Spain's cooperation with Huawei can be traced back to 2015. At the 5TONIC event hosted by Telefonica and IMDEA Networks, six suppliers including Huawei were tested to confirm a wireless transmission SDN proof of concept. On November 22, 2016, Telefonica and Huawei issued the world's first proof-of-concept for 5G user-centric and Unconventional Computation and Natural Computation (UCNC) RAN architecture. Since then, the cooperation between Huawei and Vodafone in 5G has progressed smoothly. In 2018, they jointly reached a 5G telecommunication standard and installed 5G network nodes in Madrid. As of June 15, 2019, Vodafone has launched commercial 5G networks in 15 Spanish cities with Huawei's help. In December 2019, Telefónica authorized Huawei to participate in the construction of Spain's 5G core network. As of May 13, 2020, 21 Spanish cities have activated 5G networks, and Vodafone has signed a contract with Huawei to provide 1 Gbit/s broadband services to 4 million enterprises.

Orange Spain aimed to become the second largest 5G provider after Vodafone in Spain by planning to deploy networks in Madrid, Barcelona, Valencia, Seville and Malaga in September 2020. Orange plans to increase the 5G penetration rate to 40% in 2021, 70% by the end of 2022, 90% in 2023, and 95% in 2024. Orange Spain intends to first use a 60 MHz NSA 5G network in the 3.6 GHz band, similar to the Vodafone's network, but to introduce 100 MHz as soon as possible. At present, Orange Spain has chosen ZTE as a 5G supplier partner. In the future, it may also develop deeper cooperation with other Chinese companies.

(4) The Influence of the United States

Spain has close economic, diplomatic, and military ties with the United States and sees the US as its most important non-European partner. However, Spain has shown strong independence and autonomy when it comes to 5G development. It seems less effected by US pressure than other European countries.

On July 20th, the director of the Chinese Policy Observatory Xulio Rios issued a statement criticizing the US's policy on Huawei. In the essay titled *Huawei and the Mantra of Security,* Xulio Rios said the United States has no evidence to prove that Huawei 5G will pose a security threat to other countries and that no potential security problems had been found in Huawei's equipment and technology thorough investigation by Spanish experts. He went on to state that the US's ban on Huawei and campaign in Europe to follow such measures were solely intended to restrict technological development in China. He finally recommended that European countries take prudent measures to avoid falling into the "American trap."

In July 2020, the US National Security Advisor Robert O'Brien met with his counterparts from France, Italy, the United Kingdom, and Germany in Paris to urge European countries to exclude Huawei from the European 5G network. However, Spain stated that, according to the investigation conducted by the Spanish National Intelligence Agency in June, Huawei's software fully complies with all of their relevant legal conditions and did not pose any security risks. Moreover, Spain emphasized that Telefonica's use of Huawei equipment in its 4G core network several years ago would make it difficult to exclude Huawei from the from the 5G core system, especially when it came to transmission roaming and network intelligent services. Telefonica planned to continue using Huawei's antennas, passive equipment, and other infrastructure in the 5G core and sensitive technologies such as information storage, maintaining relevant technical cooperation with Huawei. Spain also announced it intended to authorize other suppliers such as Ericsson and Nokia to avoid relying too much on a single country or company.

In recent years, Spain has developed friendly relations with China, hoping to become China's largest partner in Europe. However, the US's economic, diplomatic, and military influence on Spain should not be underestimated. The US remains Spain's largest foreign investor and the second largest destination of Spanish foreign direct investment. Spain is also one of the US's security allies, hosting two US military bases within its borders. The US plans to increase its military presence in Spain by increasing destroyers and military personnel. Finally, many Spanish foreign policy elites are inextricably linked to the United States. With intensifying economic competition between China and the United States and the deteriorating economic situation in Europe, Spanish political and economic elites tend to view China as a competitor, and they are more concerned about China's economic development model, geopolitical ambitions with the "Belt and Road" initiative, and human rights issues. In the future, these problems are likely to affect the 5G field and become unfavorable factors in cooperation between Spanish and Chinese telecommunications and technology companies. Meanwhile, the United States will continue to lobby, and may even use military and foreign policy chips to threaten Spain to stop 5G cooperation with Chinese companies.

3.1.5 United Kingdom

(1) National Security Legislation

The British Parliament promulgated a new version of the Data Protection Act in 1998, which clarified the rights, obligations, and responsibilities of data controllers in the processing of personal data, and proposed that citizens have the right to obtain data related to themselves. The basic laws in the field of information disclosure in the UK include the Freedom of Information Act (FOIA) promulgated in 2000, and the Protection of Freedom (PFA) promulgated in 2012. To strengthen network and information security, the British government issued National Cyber Security Strategy (NCSS) documents in 2009, 2011, and 2016.

In May 2019, 5G was officially launched in the UK. At first, only two operators, EE and Vodafone, provided 5G products. However, now all four major operators in the UK provide 5G services, but coverage is still limited to specific areas.

(2) 5G Construction and Designation of High-Risk Vendors

On January 28, 2020, British Prime Minister Boris Johnson chaired the National Security Council (NSC). The NSC decided to allow Huawei to participate in the UK's 5G network construction to a limited extent. However, at the same time, the NSC agreed that the National Cyber Security Centre (NCSC) would issue guidance on dealing with high-risk vendors to British

telecom operators. The so-called "high-risk vendors" would have to face a series of restrictions. Such vendors were to be:[38]

- Excluded from all safety related and safety critical networks in Critical National Infrastructure
- Excluded from security critical 'core' functions, the sensitive part of the network
- Excluded from sensitive geographic locations, such as nuclear sites and military bases
- Limited to a minority presence of no more than 35 per cent in the periphery of the network, known as the access network, which connect devices and equipment to mobile phone masts

Within the current UK legal framework, NCSC is the UK's cyber threat technology authority. As part of the Government Communications Headquarters (GCHQ), it plays multiple roles in the Security of Network and Information Systems Regulations (NIS) in the UK. It serves as a "Computer Emergency Response Team" to monitor incidents, provide early warning, disseminate information, conduct cyber threat assessments, and provide general technical support to the competent authorities. At the same time, it is also a "single point of contact" (SPOC), which receives information related to NIS events from all competent authorities and coordinates with counterpart agencies in other member states.

According to the guidance issued by the NCSC, the Chinese telecommunications manufacturer, Huawei, is classified as a high-risk supplier. Huawei was classified as high-risk for the following reasons:

- Huawei has a significant market share in the UK already, which gives it a strategic significance;
- it is a Chinese company that could, under China's National Intelligence Law of 2017, be ordered to act in a way that is harmful to the UK;
- we (NCSC) assess that the Chinese State (and associated actors) have carried out and will continue to carry out cyber attacks against the UK and our interests.
- Our (NCSC's) experience has shown that Huawei's cyber security and engineering quality is low and its processes opaque. For example, the HCSEC Oversight Board raised significant concerns in 2018 about Huawei's engineering processes. Its 2019 report confirmed that "no material progress" had been made by Huawei in the remediation of technical issues reported in the 2018 report and highlighted "further significant technical issues" that had not previously been identified; and
- a large number of Huawei entities have been included on the US Entity List for over 12 months now. Those restrictions keep tightening in a way that is likely to have an impact on future availability and reliability of Huawei's products.

In addition to NCSC, the British government uses Telecoms Security Requirements to establish safety requirements. The purpose of TSR is to strengthen the security of the telecommunications industry and reduce potential risks. It applies to both traditional fixed network manufacturers and operators using 4G and 5G mobile networks. It should be noted that TSR contains a set of regulations for identifying and restricting HRVs and their market

[38] *NCSC advice on the use of equipment from high risk vendors in UK telecoms networks*, https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

share. If an operator is concerned that a supplier's product does not comply with the TSR, it tends not to choose the HRV product, and competing manufacturers will gradually consume the HRV's market share. In addition to putting pressure on suppliers, TSR also directly prohibits HRV products in certain "core" network functions. This prohibition includes both fixed and mobile networks; it prohibits the use of certain equipment from HRVs in locations such as government departments and in various types of infrastructure.

In terms of FTTP and 5G networks, TSR has set a series of upper limits on HRVs' products as a proportion of the entire network, and this is calculated using various metrics: For FTTP and other gigabit and higher capable access networks, at most 35% of premises passed by a network should be served by equipment from an HRV ; For 5G access networks, at most 35% of expected network traffic volume on any particular network passes through HRV equipment and at most 35% of base station sites nationally on any particular network should be served by equipment from an HRV; For any other functions in 5G, FTTP and other gigabit or higher capable fixed access networks, at most 35% of the network elements from a particular equipment class in any particular network should be provided by an HRV. Finally, operators should only use an HRV if that HRV has in place a specific risk mitigation strategy, designed and overseen by the NCSC.[39]

(3) Pressure from Various Parties and American Influence

The COVID-19 pandemic, coupled with the promulgation of the Hong Kong National Security Law, has precipitated a rise in anti-China sentiment in British political circles, and MPs increasingly put pressure on Prime Minister Johnson. Under pressure from all parties, the British government finally decided to exclude Huawei from Britain's 5G construction. Besides domestic pressure, the final decision was greatly influenced by pressure from the United States. The country's government could have achieved the goal of "delivering full fibre [broadband] to every home in the land" at low cost, as promised by Prime Minister Johnson, if only the United States has not repeatedly lobbied the British government to exclude Huawei.

The US sanctions eventually forced the UK to reverse its January decision about Huawei. The British government's previous decision of allowing the use of a limited amount of Huawei 5G equipment did not satisfy the United States. On July 14, the United States issued a statement congratulating the United Kingdom on the resolution by its government to ban Huawei from entering its 5G network and to phase out existing Huawei equipment. The United States view this as a victory in its diplomatic efforts to unite with "free countries" to block Huawei completely.

According to the report by the US State Department on the Clean Network Plan, Telefónica UK (O2), which accounts for about 20% of the mobile market, has joined the plan. The decision to join the plan by the French telecom company Orange, which also has an extensive business market in the UK, may also have an impact. Besides, British Telecom (BT) and mobile market giant Vodafone, which account for about 40% of the fixed telephone market, also require the government to remove Huawei's equipment from 5G facilities by 2030.

3.1.6 Finland

(1) Finnish Cybersecurity Strategy

In 2013, the Finnish Security Council and the Ministry of Defence issued the "Finnish

[39] *NCSC advice on high risk vendors in UK telecoms*, NCSC, https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks#section_6.

National Cyber Security Strategy", which clarified several strategic objectives, including the establishment of an effective collaboration model between the authorities and other actors to promote national cyber security and cyber defense; improving the comprehensive understanding of the state of cybersecurity among key participants in important functions of society; maintaining and improving the capabilities of enterprises and organizations that provide essential services, so that they can detect and eliminate cyber threats and become more resilient to disruptions; and making cyber threat detection a part of such organizations' continuous management.

After 2016, the Ministry of Transport and Communications formulated the Finnish Cyber Security Strategy, proposing that Finland formulate competitive and progressive laws from the perspective of digital business. Finnish companies will be required to comply with international standards for information security, and the authorities will help communities and citizens improve information security.

(2) Existing Certification Standards

Regarding network security, Finland has adopted a labeling system to help authenticate equipment safety. At the end of 2019, the Finnish Transport and Communications Agency Traficom announced the use of this new label system to authenticate the security of IoT devices. This also made Finland the first European country to issue cyber security labels to network-enabled smart devices. The government will provide security labels to networked smart devices that meet the EN 303 645 certification standard, which is a consumer IoT network security standard launched by the European standards organization ETSI (European Telecommunications Standards Institute). The head of the Finnish National Cyber Security Center believes that the labeling system will allow consumers to identify secure devices and simplify their purchasing decisions.

Regarding 5G, Finland currently does not specify detailed laws to restrict operator choices. However, in 2019, the Finnish National Cyber Security Center (NCSC) announced the audit standard for cloud services, the Cloud Service Security Evaluation Standard (PiTuKri). The standard sets security standards for cloud service vendors in terms of personnel security, personal security, telecommunications security, identity and access management, information system security, encryption, operational security, portability and compatibility, change management, and system development. The draft of this standard refers to a number of international cloud service technical standards such as BSI and CSA.

(3) The Influence of the United States

Politically, Finland is currently unaffected by the United States. Although the US government hopes to support Nokia (a Finnish company) and Ericsson (Swedish) against Huawei, and there has even been speculation that the United States will invest in these two major equipment manufacturers, it has not actually taken any specific actions. For now, the Finnish government has not put forward any specific ideas for banning manufacturers from other countries.

3.1.7 Denmark

(1) Denmark's 5G Legislation

Denmark has not made specific legal regulations for 5G networks, and operations mainly rely on three relevant laws: *Act on Electronic Communications Networks and Services, Executive Order on the Provision of Electronic Communications Networks and Service, Digital Information Database Administrative Order*. The Danish legal regulations in this field generally follow the EU's legislation and regulations, while also including more detailed regulations on

the qualification review of telecommunication service operators.

At present, Denmark's 5G construction strategy mainly relies on two major policy documents: *5G Action Plan for Denmark* and *Digital Strategy 2016-2020*.

At the beginning of 2019, the Danish government released the *5G Action Plan for Denmark*, which clearly stipulates the frequencies, roll-out, regulation and use cases of 5G networks. It is now the main policy basis for the deployment of 5G networks in Denmark. The Danish Energy Agency has auctioned the 700 MHz, 900 MHz and 2300 MHz frequency bands. The Ministry of Public Utilities and Climate has decided to start auctions for the 3.5 GHz and 26 GHz frequency bands, which will be completed by 2020 at the latest. The Danish Energy Agency is the core department for 5G rollout. It has strengthened its cooperation with the Danish Competition and Consumer Authority and a number of telecommunications companies on network sharing issues, and has strengthened cooperation with municipalities, local governments and the telecommunication industry on standard setting and case guides. In terms of making the necessary regulatory preparations for 5G, the Danish government has seriously summed up the lessons of the past and is examining plans related to the principle of network neutrality in the 5G environment. The Danish Energy Agency, in conjunction with the Danish Business Authority and other authorities, is collecting 5G use cases and arranging seminars with the telecommunications industry and other stakeholders to jointly resolve obstacles in the use of 5G.[40]

The Danish government has always attached great importance to digital development, and is ambitious in the construction of 5G networks, striving to become a world leader in 5G networks. According to the plan, Denmark does not regard 5G networks as an isolated policy issue, but considers it something to be integrated into the national network and information security strategy. After deploying the 5G network, the Danish government will require all large enterprises and public sector organizations to use 5G networks to ensure that Denmark is at the forefront of this technology. The main task of the public sector will be to create a good environment for the promotion of 5G. At the same time, the network operation of public institutions must use advanced digital solutions incorporating 5G technology. For the business community, the Danish government requires domestic Internet companies to fully exploit the development potential of 5G, tap business opportunities and improve innovation capabilities.

The *Digital Strategy 2016-2020* led by the Danish Ministry of Finance specifies how 5G networks will be managed at all levels of government, focusing on a digital development model that combines municipal and regional administrative departments, supplemented by hospitals, public schools, universities and other public departments, as well as private enterprises, trade groups, communities, and non-governmental organizations and other actors. In addition, the Danish government also pays attention to international cooperation. In the 5G cooperation agreement released in May 2018, the five Nordic countries, Sweden, Norway, Finland, Denmark, and Iceland, stated that they would strengthen cooperation in information and communication technology and build the world's first 5G interconnection area.

In short, Denmark has always attached great importance to digital development, but before 2020 it mainly focused on the construction of basic broadband, and Denmark lags behind certain other EU countries. Although Denmark has relatively complete legislative regulations and governance mechanisms in telecommunication services, it has not issued a law specifically for 5G. At present, the *5G Action Plan for Denmark* is the state's only strategic plan for 5G deployment, and that plan takes the digital growth strategy published in 2018 as its blueprint. The plan can be seen as serving the development of the welfare state. It focuses

[40] *5G Action Plan for Denmark.* Danish Energy Agency.

on three aspects: promoting economic development, serving the citizens and protecting social safety.

(2) Denmark's 5G Regulatory Agency

The history of digital governance in Denmark can be divided into two stages: the first one was in the early 1990s, led by the research division of the government. Beginning in 1994, the head of the research department began to design a blueprint for Denmark to enter the information age. Since then, most of Denmark's digital policies have been developed around the construction of a welfare state, aiming to use new technologies to solve social inequality and ensure citizens' access to information. The second stage began around the turn of the century, and has been led by the Ministry of Finance. Since 2001, the Ministry of Finance has been in charge of a separate working group to strictly coordinate governance work, focusing on the establishment of a digital government, aiming to simplify laws and regulations, improve administrative efficiency, and establish a digital society.

In general, the Danish government attributed 5G management issues to the telecommunications industry and did not set up a separate 5G regulatory agency. Denmark's 5G management is characterized by the linkage of multiple sectors, in order to better serve the overall development of society using digital technology, and encourage companies to explore business opportunities in multiple fields such as waste data, underground infrastructure, energy, geographical factors, climate, and water resources. Currently, Denmark's national broadband construction is mainly in the hands of four agencies:

a. Ministry of Energy, Utilities and Climate, is responsible for the formulation and management of the Danish broadband policy, including the formulation of the regulatory framework for the telecommunications sector and the development of broadband construction goals.

b. Danish Energy Agency is mainly responsible for the fields of energy, utilities and climate. It is also the main national regulatory agency for Danish Telecommunication. The central task of the agency is building national broadband capacity, and it is responsible for the implementation of broadband policies, physical infrastructure, licenses, radio equipment, and other matters related to network neutrality and spectrum management.

c. The Ministry of Industry, Commerce and Financial Affairs is a lower-level organization under the Danish Business Authority, which is solely responsible for market analysis and decision-making, as well as Internet supervision and electronic privacy protection.

d. The Danish Ministry of Finance established the Danish Agency for Digitisation in 2011 in order to accelerate the digitalization process, serve the modernization of the Danish welfare society, and implement the government's digitalization goals in the public sector.

The Danish Energy Agency and the operator TDC are the two major organizations promoting 5G technology. The former is responsible for the supervision and regulation of 5G networks, and the latter is responsible for implementing the planning goals of 5G development in Denmark at the commercial and technical levels.

(3) Denmark's Qualification Review for 5G Service Providers

Act on Electronic Communications Networks and Services defines "provider" as: "any person who makes products, electronic communications networks or services governed by this Act available to other parties on a commercial basis"[41]. This includes not only traditional telecommunications companies that provide Internet access and voice phone services, but

[41] *Act on Electronic Communications Networks and Services* (English translation)

also other enterprises, organizations, and institutions that provide electronic communication networks or services as their main activities. It is worth noting that the criterion in this definition lies in "commercial basis" rather than "commercial purpose." In other words, if an entity's activity is usually based on commercial activities, then it is regarded as a "service provider" and is subject to the corresponding legal constraints, regardless of whether the goal of the enterprise, organization, or institution is to obtain profit. According to the Danish Telecommunications Regulations, providers of electronic communication networks and services do not need to be authorized, but must be registered in the telecommunications center of the Danish National Police.

Since October 2018, in order to optimize the use of taxpayers' money, Denmark has adopted a public bidding process for services in the digital field. The bidding process involves three major areas: usage standards, technical requirements, and public supervision, in order to minimize transaction costs and ensure that bidders meet Danish and international data requirements standards. In short, the infrastructure construction of Denmark's 5G network is based on market-oriented principles, and the public sector is responsible for ensuring information security and providing a regulatory framework. The security review of 5G equipment vendors includes two aspects: market selection and government investigation. The former is based on consumer demand and puts forward technical requirements for 5G equipment vendors; the latter aims at national and social security and tends to select 5G from equipment vendors based in allied states.

1) Technical Requirements

At present, the biggest obstacle standing between Denmark and 5G network is the lack of infrastructure. The country's infrastructure will require a lot of expansion, the establishment of more new antenna poles and a revision of antenna positions. With the infrastructure in place, mobile network providers will be able to develop and operate public networks. Therefore, mobile network providers need to meet the following technical conditions:

a. Have good and stable working conditions.

b. Have the ability to expand infrastructure in Denmark.

c. Be able to complete the work described above at low cost.

According to the *Act on Electronic Communications Networks and Services*, the Danish government pursues the principle of "technological neutrality" in the management of telecommunications. That is, the services involved, no matter whether it is a mobile network or a fixed network, are treated the same in management without distinction. The same applies to 5G construction. At the same time, the Danish government focuses on the wishes of consumers. Only when the demand is high enough, will more funds be invested in the large-scale expansion of 5G networks.

2) Security Review

According to Reuters, Denmark hopes to introduce 5G suppliers from allied countries or countries with close ties. Companies from countries that are not from security allies will be excluded from critical infrastructure services.[42] Minister of Defence Trine Bramsen said in an interview that "In order to protect Denmark and the Danes, we want to collaborate with someone with whom we already have alliances."

[42] *Denmark wants 5G suppliers from closely allied countries, says defence minister*, Reuters, JUNE 8, 2020. https://www.reuters.com/article/us-telecoms-5g-denmark/denmark-wants-5g-suppliers-from-closely- allied-countries-says-defence-minister-idUSKBN23F1IT

Last year, TDC, Denmark's largest single telecommunications operator, chose Ericsson for 5G network deployment. As China is not a security ally of Denmark, Huawei will not be able to provide Denmark with critical infrastructure. Up until now, Huawei's technology and equipment have been widely used in mobile networks in Denmark. The established practice of TDC is to use Huawei in the mobile network and Ericsson in the core network. In addition, Nordic telecoms 3, Telia and Telenor have not yet identified suppliers for their 5G development in Denmark.

(4) American Factors in the Development of 5G in Denmark

1) Due to the threat from the United States, Denmark abandoned its original strategy of cooperating with Chinese telecom companies.

Initially, the Danish government preferred to cooperate with Huawei to develop 5G networks, but due to the influence of the United States, it ultimately changed its policy direction.

On May 3, 2018, TDC cooperated with Huawei to jointly test 5G technical standards on the 100MHz spectrum in the 3.5GHz band granted by the Danish Energy Agency, and successfully reached a transmission speed of 1.9Gbps. But on May 9, TDC suddenly announced that it would replace Huawei with the Swedish company Ericsson for 5G mobile network services. In just a few days, the Danish government's attitude towards Huawei took a turn for the worse, largely because the United States publicly asserted that Huawei had engaged in intelligence cooperation with the Chinese government, in the future would use its 5G network equipment to disclose the data it has to the government and conduct espionage activities. At the same time, the United States also roped in its allies to put pressure on the Danish government. For example, Germany has warned that if Denmark uses Huawei's equipment in the 5G infrastructure, the amount of sensitive information Germany shares with Denmark will be reduced. Various forms of pressure exerted by the United States have forced Denmark to stop 5G cooperation with Chinese telecom companies.

On December 19, 2019, Greenland, an autonomous territory of Denmark, decided to replace Huawei with Ericsson to provide equipment for its 5G telecommunications network. At that time, the United States was working to persuade allies to jointly reject Huawei's 5G technology. In August, Trump even threatened to purchase Greenland from Denmark as part of the US strategy to enter the Arctic. The United States used such "carrot + stick" approach to force Greenland gave up its 5G cooperation with Huawei.

Since then, the Danish Minister of Defense officially announced that it would introduce 5G vendors from security allies. The United States highly praised Denmark's action. The US thought that only allowing "trusted 5G suppliers" could effectively protect national security. According to US standards, Chinese companies such as Huawei and ZTE are both "untrusted IT vendors". As it stands, Denmark appears to have abandoned its strategy of cooperating with Chinese vendors on 5G.

2) Despite Threats from the United States, Denmark May Still Avoid Interference.

The goal of Denmark's 5G plan is ambitious, as it aims to become a world leader in 5G, but compared to 5G development of many of its EU neighbors, Denmark is a late bloomer. It is still in the testing phase, and it may be several years before the higher frequency bands can be used by mobile communication companies. At the same time, only if consumers have enough demand can Denmark be able to further develop 5G technology. In other words, the basic technology for 5G development in Denmark is still immature and will require a long time to prepare. Therefore, there are still many variables in future development. Coupled with the willingness of cooperation in Denmark, there is still the possibility that Denmark will cooperate

with Chinese vendors on 5G deployments in the future.

Of the 147 cities in the EU where 5G has been deployed, only two of them — Copenhagen and Aalborg — are in Denmark. These two cities have established 5G private pilots, 5G test corridors and infrastructure. Denmark's 5G development is still in its infancy and the country still lags behind its EU neighbors. Specifically, there are two major issues:

First, Denmark has not reached the 5G technical standards in the appropriate frequency band. Currently, the European Union has allocated the 700 MHz frequency band to seven member states: Germany (2015), France (2015), Finland (November 2016), Hungary (2020), Italy (2018), Sweden (2018), and Denmark (2019). Of these seven, only Denmark has not yet reached the EU standard for the use of 5G technology in the 3.6 GHz frequency band. It is expected to auction higher frequency spectrum in 2020 and complete the 26 GHz high frequency spectrum auction in the third quarter. On April 4, 2019, Denmark completed auctions of 700, 900 and 2300 MHz frequency bands. The buyers were TDC, Hi3G and TT-Netvaerket, and the auction raised a total of 2.21 billion Danish kroner (296 million euros).[43] The license is valid for April 2020. According to the *5G Action Plan for Denmark*, the 3.5 GHz band is expected to be available in 2020. It is expected that 5G will be launched after the 26GHz frequency band is put into use.

Second, the development of 5G in Denmark faces many commercial and technical challenges. The initial spectrum bidding method is effective, and the strong domestic operators and mature IT industry provide a driving force for the development of 5G. However, Denmark still needs to overcome many shortcomings, such as the lack of test licenses, the relatively late launch of 5G in the country, the inability of existing public networks to support 5G promotion, limited financing, and low initial demand.

3.1.8 Sweden

(1) Sweden's National Cyber Security Strategy

In 2017, the Swedish Ministry of Justice issued the "National Cyber Security Strategy", which clearly stated that a complete set of cyber security strategies should be established. The purpose is to help create long-term conditions that allow all stakeholders in society to effectively commit to cyber security and improve the overall awareness of cybersecurity in Swedish society. The government hopes to support efforts and participation in the community to enhance cyber security. The strategy names six major issues as priorities for improving the level of cyber security, including ensuring systems and comprehensive cyber security methods, enhancing the security of networks, products and systems, enhancing the ability to prevent, detect and manage network attacks and other IT incidents, and prevent and combat the possibility of cybercrime, increase awareness and promote professional knowledge, and strengthen international cooperation.

The Swedish government has imposed restrictions on companies and institutions use of cutting-edge technologies through the EU's General Data Protection Regulation (GDPR), and the Swedish implementation imposes stricter standards than the EU regulation requires. In 2019, a Swedish high school became the first organization to be fined by the Swedish Data Inspection Authority (DPA) under the EU's General Data Protection Regulation (GDPR). The high school was ordered to pay 200,000 Swedish kronor (approximately 148,000 yuan). The school uses a facial recognition system to record the attendance of students. The Swedish DPA

[43] *Denmark completes auction of the 700 MHz band*, 5G Observatory, https://5gobservatory.eu/denmark-completes-auction-of-the-700-mhz-band/.

conducted a survey of 22 students involved during the system's trial and determined that the school board's processing of students' personal information did not comply with GDPR regulations. In 2020, Google Inc. was fined 8 million U.S. dollars for violating data protection laws in Sweden. Based on a four-year investigation in Sweden, it was determined that Google had violated the provisions of the GDPR. When a user deletes search results, Google has no right to notify any other third party about the user's actions. In addition to imposing fines on Google, Sweden further required Google to refrain from informing website operators that their URLs will be de-indexed.

(2) Interpretation of 5G Policies and Regulations in Sweden

In 2018, the world's first 5G phone call was made from the Kista laboratory of the Swedish telecom company Ericsson. In December, the Swedish telecommunications regulator announced the completion of the first round of 5G 700M spectrum auctions. Ericsson and the pan-European telecommunications company Telia jointly pressed the 5G network start button at the Royal Institute of Technology (KTH), marking Sweden's first adoption of a standard 5G network. There are plans to provide 5G coverage on a large scale throughout the country before the end of 2020.

According to reports from Reuters and Sputnik in 2019, the Swedish government tried to formulate a new law in 2019, "Protecting Sweden's Security During Radio Use" (Skydd av Sveriges säkerhet vid radioanvändning). The law was passed by the Swedish House of Representatives at the end of 2019.

This law was recommended by the Ministry of Infrastructure to the Council on Legislation on August 30, 2019. The Council on Legislation recommended amendments to the "Electronic Communications Act" and the "Public Access to Information and Secrecy Act" to enhance the security of Sweden's use of radio transmitters. Under the amended law, parties applying for a license to use radio transmitters or to obtain consent to transfer or lease such licenses must meet the condition that it can be assumed that the use of radio will not harm Sweden's security. In addition, the granting of permits must take into account requirements closely related to Sweden's security. If it is determined that the use of radio may harm the country's security, the license must be revoked or the license conditions changed immediately. These regulations do not apply to broadcasting licenses that require a license under the Radio and Television Act. The Swedish Armed Forces and Security Police (SÄPO) must be able to appeal decisions on permit issues affecting Sweden's security. It is also recommended that the Swedish Post and Telecommunications Agency, the security police and the armed forces can exchange necessary information on licensing issues related to Sweden's security.

3.1.9 Poland

(1) Laws Related to the Internet

a. Amendment to The Development of Telecom Services and Networks Support Act

Currently, Poland has no specific legislation in the 5G field. The latest authoritative legislation is the Amendment to The Development of Telecom Services and Networks Support Act, or the so-called Mega-Act. The first version of the bill was launched in May 2010 and was amended in August 2019. The content includes the Telecommunications Law (2004), the Construction Law, and the law on Public Roads. The amendment is intended to make it easier for telcos to expand services to areas where it would currently be unprofitable to roll out

infrastructure by eliminating some of the administrative and legal barriers.[44] Additionally, the Act on Competition and Consumer Protection of February 16th 2007 (ACCP) and the Personal Data Protection Act of May 10th 2018 are also seen as supplemental documentation to the Mega-Act.

i. The Mega-Act indicated that the most important regulator of the ICT industry is the Office of Electronic Communications (UKE), Poland's Telecommunications regulation institution for telecommunications, postal activities and spectrum resource management. Along with the Office of Electronic Communications are the National Broadcasting Commission, the Office of Consumer Protection and the Office of Personal Data Protection.

ii. The Telecommunications Law identifies telecommunications activities that are regulated, specifies the form of a "license" in the management of spectrum and numbered resources (Art. 114 of the Telecommunications Law), and gives the President of the UKE the power to restrict the access of entities. According to the law, in the absence of adequate frequency resources, the entity to be granted the generic exclusive frequency license shall be determined by means of competition, bidding or auction (Art. 116 of the Telecommunications Law). The use of radio equipment requires a license issued by the President of the UKE (Art. 143 of the Telecommunications Law). When it is in the public interest to do so, the president of the UKE may reserve a specified frequency, define the conditions of a tender or auction, and in particular identify entities not entitled or entitled to participate in a tender, (Art. 118 of the Telecommunications Law). The President of the UKE has the power to refuse a permit he or she deems it a threat to national security and public order.

iii. The Telecommunications Law holds telecom enterprises responsible for protecting privacy and data security. Under the provisions of the Telecommunications Law and other regulations, telecommunications enterprises must fulfill certain obligations regarding national defense, national security and public order. They are obligated to keep a record of what users send and receive, and to provide data support when security and border guards need it.

iv. The President of the UKE has taken a series of measures to promote 5G technology in Poland. In addition to supporting the Mega-Act, the President of the UKE has developed concepts to improve the efficiency of spectrum use, and redistribute and optimize spectrum resources. In addition, 5G work has been promoted through Poland's active participation in the International Telecommunication Union (ITU), meeting of the European Post and Telecommunications Authority (EFTA), and relevant organizations operating within the EU (such as the Radio-Spectrum Commission, Radio-Spectrum Policy Group and Communications Commission). In April 2019, the President of the UKE announced an action plan for the 3600-3800 MHz band. Currently, the Ministry plans to revise the Telecommunications Law and add a list of requirements that participants must meet to participate in 5G frequency bidding.

b. National Cybersecurity Systems Act

On August 28 of 2018, Poland's National Cybersecurity Systems Act (KSC) came into effect. It is the first Polish Act to systematically identify the department responsible for cybersecurity. The purpose of the act is to prevent cybersecurity risks. It involves the organization of national cybersecurity systems, the tasks of various departments, and the ways in which the law is monitored. Its main provisions include[45]: 1) the establishment of a computer security incident response team under the NIS directive of the European Commission, 2) the establishment of

[44] *Poland amends telecoms Mega-Act*, 17 May, 2019, https://www.commsupdate.com/articles/2019/05/17/poland-amends-telecoms-mega-act/.

[45] *Guide to JST Act on national cybersecurity system*, https://www.gov.pl/documents/31305/436699/Poradnik_dla_JST_ustawa_o_krajowym_systemie_cyberbezpieczeństwa.pdf/86096d16-1193-e277-aff2-ddd5db0db647

an effective ICT security system, and 3) the strengthen information exchange with the EU.

The establishment of a single point of contact within the Digital Services division aims to collect information on cyber security incidents nationwide and to exchange information across borders with similar institutions in other countries. (If CSIRT receives an alert of a serious incident that could affect at least two EU member states, they will be able to alert other EU member states through contact points.)[46]

If an entity provides critical services in other EU member states, the competent authorities in the administrative process shall consult with those states through a single point of contact to determine whether the entity is recognized as a key service operator in those states.[47]

(2) National Security Strategy of 2020

The National Security Strategy of Poland was signed by the President on May 12, 2020. The strategy calls for the development of domestic solutions in the field of cyber security, as well as in other fields of modern technology (including machine learning and the Internet of Things); and it encourages state-funded research and development work to inspire domestic potential in developing fixed and mobile broadband networks (5G and its successors), including partnerships with universities, research institutions and enterprises in both the public and private sectors.

The development of solutions based on fixed and mobile broadband (5G and its successors), the Internet of Things, cloud computing, quantum technology, service automation, machine learning, nanotechnology, and artificial intelligence has created new opportunities for Poland's development while also posing previously unknown threats. In the context of the digital revolution, the specific role of cyberspace and information space should be fully considered. The availability of broadband internet also creates a space for disinformation and manipulation of information, and effective strategic communication activities are required to counter that.[48]

At the strategic level, capabilities should be established to protect the information space, including the elimination of disinformation, and these capabilities should be understood as the integration layers of the space: the virtual layer (systems, software and application layers), the physical layer (infrastructure and equipment layers), and the cognitive layer. A unified national strategic communication system should be established, whose tasks should include the use of a wide range of communication channels and media to predict, plan and implement coherent communication activities, and the application of identification and impact tools in all areas of national security.

(4) Influence from the US

On September 2, 2019, the Prime Minister of Poland and vice President of the US signed a joint statement about construction of 5G networks, to strengthen cooperation between Poland and the US in the field of 5G development, and also to exclude some enterprises from participating in the construction of 5G networks in Poland.

The statement says 5G networks must be based on free and fair competition,

[46] *The Act on the National Cybersecurity System has entered into force, Service of the Republic of Poland*, August 28, 2018, https://www.gov.pl/web/cyfryzacja/ustawa-o-krajowym-systemie-cyberbezpieczenstwa-weszla-w-zycie

[47] *COMPETENT AUTHORITY – who is it?*, Service of the Republic of Poland, https://www.gov.pl/attachment/5e29da7b-db2a-4a58-9c68-15caf4b5c815.

[48] *National Security Strategy of the Republic of Poland 2020*, pp7-8. https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf,

transparency and the rule of law and that, in order to protect communications networks from disruption or manipulation, it's important to make sure that only reliable and trustworthy enterprises participate in the construction of networks. The statement puts emphasis on the privacy and personal freedoms of the citizens of the country. Poland conducts careful and thorough evaluation of hardware and software manufacturers. A careful assessment of a 5G enterprise pays attention to the following elements:

a)Whether the supplier is controlled by a foreign government, and whether it has recourse to an independent court

b)Whether the supplier has a clear ownership structure

c)Whether the supplier has demonstrated ethical corporate behavior in its history, and whether it complies with legal requirements to ensure transparency in corporate activities.

Poland's Prime Minister published an article in The Daily Telegraph on July 15 of 2020, named "All of Europe must stand with America on 5G". The article asserts that 5G is the key technology of future economic development, and 5G network and the supply chain should be operated by enterprises that are under the government's control. He called for a more united alliance among the European countries and the US in the development of 5G technologies. According to the Prime Minister's article, Poland must ensure that it can confront the risks and vulnerabilities posed by 5G progress and build a 5G ecosystem based on trust and responsibility.

Recently, exchanges between Poland and the US have become more frequent and bilateral relations have become closer. During U.S. Secretary of State Mike Pompeo's visit to Poland in August 2020, the two sides signed the Strengthening Defense Cooperation Agreement.

3.1.10 Estonia

(1) National Cybersecurity Strategy

Estonia was hit by a series of massive cyber-attacks that began at the end of April 2007. The attacks, which targeted congress, government agencies, banks, and media sites, were widespread and intense. Many people seem to believe that the cyber-attack was carried out by Russia. Affected by this incident, Estonia published its first National Cybersecurity Strategy in 2008, which indicated that cybersecurity has become an important part of its national security. This document drafted by the Defense Department, notes the interdisciplinary nature of cybersecurity and stresses the need for coordinated efforts on a regional scale. Subsequently, Estonia released two versions of its National Cybersecurity Strategy in 2014 and 2019 respectively. The document was drafted by the Ministry of Economic Affairs and Communication rather than the Ministry of Defense, which indicated that Estonia will improve its information security capabilities and develop critical infrastructure rather than just dealing with cyber-attacks. As shown in Table 6, Estonia focuses on international cooperation related to cybersecurity within the framework of the EU and NATO, and promotes cooperation with strategic international partners. Thus, geopolitics is becoming an important factor in Estonia's cybersecurity construction.

	The 2008-2013 Edition	The 2014-2017 Edition	The 2019-2022 Edition
Department	Ministry of Defense	Ministry of Economic	Ministry of Economic

in charge of drafting		Affairs and Communication	Affairs and Communication
Core of the Strategy	Develop and implement security measures on a large scale; Improve the legal framework that supports cybersecurity; Enhance network security capabilities	Protect critical infrastructure; Crack down on cyber-crime; Improve information security capabilities	Build a sustainable digital society; Develop a network security industry; Become a leading contributor globally;
International Cooperation	Participate in the work of international organizations: UN, EU, OSCE, NATO, OECD	Work with Allies, partners, and like-minded nations	Work with strategic and key partners; Main framework: EU, NATO

Table 6 Estonia's National Cyber Security Strategy of Estonia

(2) Government Department and Organizational Structure

In 2009, the Cybersecurity Council was established under the administration of the government's Security Committee. The Council's main task is to promote inter-agency cooperation and monitor the implementation of strategic cybersecurity objectives. The cybersecurity committee is chaired by the secretary general of the Ministry of Economic Affairs and Communications, and the two executive branches cooperate confidentially. In addition, another important position in its national cybersecurity governance is the national Cybersecurity Policy Director who is responsible for leading the formulation and implementation of cybersecurity policies and strategies. Raul Rikk, who has been in charge since 2019, gave a glimpse of the latest legislative trends in Estonia through his recent remarks on 5G laws and regulations.

(3) Related Telecommunications Bills and the Latest Legislative Trends

i. Electronic Communications Act and the Amendment

In 2004, Estonia passed the Electronic Communications Act, which sets out clear requirements for communication service providers in Chapter 8. And it specified the requirements for communications services and communications networks provision as well as the quality of communications services in Section 87.

a. When providing communication services, communication enterprises shall follow these principles and objectives:

- Ensure the security of communication network operations;
- Maintain the integrity of the communication networks;
- Ensure the protection of transmitted or stored information;
- Ensure the interoperability of communication networks and services;

- Meet safety and environmental requirements;
- Meet the urban planning and land adjustment requirements;
- Ensure the quality of communication services;
- Avoid harmful and interfering effects from other space-based or ground-based technology systems;
- Ensure public order and national security;
- Supervise compliance with applicable requirements, the submission of information, and the organization of statistics;
- Avoid actions that may harm the free competition of the communications market.

b. In accordance with the principles and objectives set out in Paragraph 1 of this section, the national government may set up technical requirements for communications networks and services provision for the following purposes:

- Protecting users;
- Publishing relevant user information through directory inquiry and relevant services;
- Ensuring that a connection is established with the national emergency telephone number in addition to the European emergency telephone number "112" and locating emergency telephone number callers;
- Ensuring public order and national security;
- Providing communication services for people with special needs;
- Connecting and ensuring operations of communications network interoperability;
- Determining the location of interconnection points;
- Promoting and ensuring connections with the pan-European 116 helpline.

c. Communications enterprises must provide information on their websites about the quality of communications services they provided to end users and measures taken to ensure equal access to end users with disabilities; otherwise, they should find a comparable alternative.

d. The service provider whose services shall be used by at least 10,000 end users shall be the provider of the essential services specified in the Emergency Law in accordance with Article 36.1 (5)–(7).

e. Multiplexing service providers and communication enterprises providing cable distribution services shall be universal service providers as they are referred to in the Economic Activities Code Act.

The amendment in 2014 added a new clause under Article 87 of Chapter 8, authorizing the technical supervision institution to require suppliers to conduct security audits, specifying as follows:

- Provide information needed to assess the security and integrity of its communication services and networks, including security policies;
- Arrange for a security audit to be conducted by a qualified independent body or

national authority and the results thereof to be provided to the Estonian Information Systems Authority. The communications company shall bear the cost of the audit.

The amendment does not specify the method and standard of the security audits, which if carried out by national authorities, may deviate from a focus on security and become politicized. In the absence of clear audit standards, communications companies may face implicit discriminatory terms and unfair market competition. For example, national authorities have excluded certain communications companies for failing a security audit.

On May 12, 2020, the Estonian Parliament amended the Electronic Communications Act, adding two subsections under Chapter 8, Article 87, Paragraph 2, to make clear requirements for communication service providers:

Subsection 1 says that, in order to safeguard national security, the national government may require communications enterprises to provide information on the hardware and software used in communications networks. Notification obligations and procedures should be established and the agencies to be notified must be designated by national regulations.

Subsection 2 says that, in order to safeguard national security, the national government may require communications companies to apply for the authorization of the use of hardware and software devices. The obligations and procedures in applying for authorization shall be confirmed, and the authority shall be designated in accordance with the provisions of the national government.

The amendment gives the national government the authority to issue an administrative order requiring communications service providers to fulfill their notification obligations regarding the hardware and software technologies used in their communications networks, and it gives the government the authority to require communications service providers to apply for licenses before using such technologies. In the absence of legal provisions that protect the intellectual property rights of enterprises, the new provisions of this amendment will increase the risk of leakage of the core technology of communication suppliers.

In addition, according to the explanatory provisions of the draft regulations, reliable partners must provide communications services and establish communications networks through secure technologies in order to ensure the quality of communications network security, reduce the risk of network attacks, and prevent political manipulation. In its explanatory clause, "reliable partner" is defined relatively vaguely and is highly subjective. The Estonian government could use the clause to take geopolitical evaluation when selecting 5G suppliers, thereby turning the fair competition of the communications market into a tool for political manipulation.

ii. The Government's bill on 5G technology suppliers

The Estonian public broadcasting company Eesti Rahvusringhaaling (ERR) reports that the Ministry of Economic Affairs and Communications is drafting a bill to restrict the use of high-risk technologies on telecommunications networks. At the operational level, the bill clarified the procedures of the authorization for communications providers. In an interview, Raul Rikk, the director of Estonia's national cybersecurity policy, referred explicitly to Chinese technology as high-risk. The bill would thus limit Huawei's participation in the construction of 5G networks in Estonia.

Specifically, the act would give each communications provider a security rating that would assess whether their products are suitable for use in telecommunications installations, and allow suppliers to provide specific technologies based on different security ratings. Criteria for

security assessment include whether the supplier is a listed company and whether it is located in an EU member state. The criteria will largely limit the participation of non-European operators in Estonia's 5G network. Huawei, for example, is bound to get a lower score than Ericsson, the Swedish telecoms operator, on this criterion. The act, which claims to assess the security level of telecommunications providers, uses executive orders to exclude specific telecommunications providers and distorts market competition. If passed, the bill would also affect 5G technology networks in use, such as the possibility that Estonia's local telecoms companies may have to replace their products that are from certain suppliers.

The Estonian government has yet to announce the details of the bill, which is expected to undergo review in August, with telecoms companies submitting their own suggestions and comments. Sami Seppanen, the CEO of Elisa, one of Estonia's three biggest telecoms, has criticized the drafted version. He described the restrictions as a misguided assumption and a political move based on the security risks posed by Huawei. Completely replacing Huawei's equipment would cost 500 million euros in the short term and add extra costs for consumers. To sum up, the security rating assessment bill favors politicization over security issues and represents the future legislative trend of Estonia, indicating that the geopolitical factors have become an important policy consideration in this trend.

(4) The Trend of 5G Network Policy Politicization and Geopolitical Considerations

Because of its special geographical location, Estonia is beleaguered by geopolitics to the point it has become an important factor in its domestic cybersecurity strategy and relevant laws formulation. Estonia is heavily dependent on the US for national security and is also influenced by the US in the formulation of 5G policies. This makes it difficult for Estonia to allow Huawei to participate in the buildout of its 5G networks.

Estonia became the second EU member state, after Poland, to ban Chinese companies from providing software or hardware devices for its 5G networks. Although development through 5G is necessary for Estonia to gain innovative advantages, the national security threats presumably from Russia have necessitated the assistance of the US, which brings other pressures to the table.

Estonia was annexed by Russia in the 19th century and was part of the Soviet Union following World War II, which shows the longstanding tensions at play. In 2017, as Estonia prepared to remove its Soviet-era bronze statues, Russian government sharply criticized the move and Estonian Russians rioted. As a result, Estonia has strengthened ties with the West in response to the threat from Russia, relying heavily on the US-led NATO alliance for defense, including in the area of cybersecurity. In its three national cybersecurity strategies, the Estonian government mentions cooperation with NATO numerous times, indicating that NATO is very important to its national security. The Estonian government needs America to support its defense.

It is in this context that Estonia and the US government signed the US-Estonia 5G Security Joint Statement in 2019, in which the two governments said, "It is essential for countries to transfer from untrusted ICT providers and supply chains to trusted providers. These efforts will not only improve our national security, but will also provide private sector innovators with the opportunity to succeed in free and fair competition, which will benefit our digital economy." The joint statement restricts Estonia's use of equipment from untrustworthy suppliers in 5G core networks, effectively ruling out Chinese companies as software or hardware providers for Estonia's 5G networks.

Juri Ratas, Estonia's prime minister, commented: "We are following common principles in developing 5G networks. The credibility of new technologies as a digital nation is a top priority

for Estonia and the US is our most important ally in terms of security. This statement agreeing with the US gives a strong signal that Estonia, along with its allies, understands security in developing 5G networks."

3.1.11 Russia

The basic framework of Russia's cybersecurity strategy have come from a recent series of policies and bills on strengthening cybersecurity.

(1) Key Documents of Cybersecurity Strategy

1) "Information Security Theory"

The new version of the information security doctrine, published on December 5, 2016, aims to ensure Russia's national security in the information industry, prevent and contain military conflicts related to information technology from a strategic level, and provide a foundation and framework for the formulation of subsequent documents and bills. The document is divided into five main parts: General Principles, National Interests in the Information Field, Main Information Threats and Information Security Status, Strategic Objectives and Main Development Directions for Ensuring Information Security, and Organizational Basis for Information Assurance.

2) "2017-2019 Russian Federation Science and Technology Development Strategy"

On May 9, 2017, Russia announced the "2017-2019 Science and Technology Development Strategy of the Russian Federation". The strategy clarifies the goals and measures of its domestic and foreign policy in the field of information and communication technology, to develop the information society and national digital economy. The strategy is an important implementation plan of the Russian Federation's science and technology development strategy, which is specifically divided into two implementation stages: 2017-2019 and 2020-2025.

3) The Russian Federation Cyber Sovereignty Act and the "Disconnection" Experiment

The Russian Federation Communications Law and the Russian Federation's Law on Information, Information Technology and Information Protection was promulgated on November 1, 2019, also known as the "Sovereign Internet Law". For the first time, the bill constituted the country's sovereignty bill in international cyberspace in the form of domestic laws and regulations, and clarified the powers of national cyber sovereignty. The content of the national domain name system in the bill will take effect on January 1, 2021.

The new law aims to protect Russia from foreign restrictions by creating a sustainable, secure, and fully functional local Internet, requiring the establishment of a surveillance and management center under the responsibility of the telecommunications supervisory agency Roskomnadzor. The Supervision Bureau has the right to decide what constitutes as a threat and how to handle it. Once it is determined that the national network is threatened, the Supervision Bureau can disconnect from the external Internet, and centrally control the communication used by the public while ensuring the stable operation of the national network and the Internet. In addition, information from state entities and state-owned enterprises on the Internet will be protected by encryption.

The following month, the Russian government announced that it completed the external "disconnection" test exercise of the national Internet, to ensure that the Russian network could operate without interruption under any circumstances. The law stipulates that similar

exercises must be done at least once a year. During the exercise, the Russian Ministry of Communications and cybersecurity companies studied the cybersecurity issues of Russian power facilities, and the Ministry of Emergency Situations evaluated the level of collaboration between government agencies and the troubleshooting capabilities of communications networks.

(2) AI and 5G Related Policies and Legal Documents

1) Regulatory Concept Document in the Field of Artificial Intelligence and Robotics

On July 21, 2020, the Russian Ministry of Economic Development proposed a regulatory concept document on artificial intelligence (AI) and robotics within the framework of the federal Digital Environment Regulatory Management project of the national plan Digital Economy of the Russian Federation, and submitted relevant drafts to the government.

The Ministry of Economic Development pointed out that the main problems and legislative gaps must first be filled and resolved. At present, Russia has no specific laws and regulations outlining the use of AI and robotics. The concept mainly includes five aspects: 1. General provisions (objectives of the concept document, regulatory objectives and tasks, principles, and directions); 2. Data circulation, legal responsibilities for using AI systems and robots, the export of AI systems and robots, insurance institutions, security issues (including information security), the formulation of technical terms and definitions in the field of AI and robotics, and related international documents; 3. Strengthen the supervision of the use of technologies in various fields (e.g., pharmaceuticals, industry, transportation, government administration, and urban planning), space programs, and financial legislation; 4. Regulatory measures to financially stimulate the development of the industry, including measures for the development of public-private partnerships; 5. The implementation mechanism helps to create more favorable developments for the regulatory environment of artificial intelligence and robotics.[49] Additionally, the Ministry of Economic Development also listed "legal obstacles" to the introduction of robotics and AI technology in various fields.

2) "Russian National Artificial Intelligence Development Strategy by 2030"

On October 11, 2019, Russian President Vladimir Putin signed an order to approve the release of the Russian National Artificial Intelligence Development Strategy by 2030. This is the first time that Russia has made the development of artificial intelligence part of its national strategy. The strategy puts forward the development ideas of Russia's artificial intelligence industry over the next 10 years and clarifies the basic principles, overall goals, main tasks, work priorities, and implementation mechanisms of Russia's development of artificial intelligence. By promoting the development and application of artificial intelligence technology, Russia hopes to ensure national security, empower its economy, and gain global leadership in the field.

3) The Russian Federation Creates and Develops 5G/IMT-2020 Network Concept Document

On December 27, 2019, Order No. 923 of the Ministry of Telecommunications and Mass Communications of the Russian Federation approved the Concept Document for the Creation and Development of 5G/IMT-2020 Networks in the Russian Federation.[50] The document

[49] *The Ministry of Economic Development has developed a Concept for the regulation of AI and robotics technologies*, Ministry of Economic Development Russian Federation, July 21, 2020, https://www.economy.gov.ru/material/news/minekonomrazvitiya_razrabotalo_koncepciyu_regulirovaniya_tehnologiy_ii_i_robototehniki.html

[50] *Concept of creation and development of 5G / IMT-2020 networks in the Russian Federation*, https://digital.gov.ru/uploaded/files/kontseptsiya-sozdaniya-i-razvitiya-setej-5g-imt-2020.pdf

mainly defines the main characteristics of the 5G/IMT-2020 network by comparing it with the existing IMT network, and it also defines the basic services of the 5G/IMT-2020 network and its relevance to Russia. The document refers to the international telecommunications market trends such as establishing and using the licensed and unlicensed frequency bands of the 5G/IMT-2020 network. Furthermore, it determines the advanced requirements for building 5G/IMT-2020 infrastructure networks by referring to the virtualization of network elements and functions (SDN/NFV), cloudification of radio access technology (Cloud RAN), and transmission network virtualization (virtualized backhaul), among others.

Chapter 5 of the document clearly puts forward the requirements for software trustworthiness and key security to ensure stable functions and network availability. Specific measures include:

- For devices with 5G networks (5G-AKA and EAP-AKA' protocols) that have been mutually authenticated, use identity verification and key agreement protocols.
- Provide mandatory support for user unit (UE) and base station (gNB) from UE to gNB user, signaling RRC traffic encryption and integrity monitoring. Mandatory support for encryption and integrity of NAS signaling from UE to access and mobility control function (AMF). Use basic algorithms SNOW 3G, AES, and ZUC to perform encryption and integrity control.
- Use the hidden user ID SUCI and the world's only temporary symbol ID 5G-GUTI to ensure the confidentiality of user identity.
- Application of base station interface protection and network security domain formation.
- Based on the cryptographic mechanism of network functions AUSF, SEAF, ARPF, SCMF, SPCF, and SIDF to ensure information security for the entire network architecture.
- Build "network slices", which provide isolation of different layers of the network and define their own security level for each layer.
- Provide the possibility to realize encryption protection through the final service (V2X, IoT, IMS, etc.) running on the 5G network.
- Support the TLS protocol, so as to exchange information securely between the core functions of the 5G network.
- Apply signaling and user traffic protection between 4G-LTE eNB base stations and 5G gNB base stations.

The document also proposes that the development of 5G networks in Russia should use local encryption algorithms, as well as trusted software (SW) and trusted electronic component libraries (EEE).

In terms of ensuring the security of 5G networks, document requirements include: preventing unauthorized access to critical and important information, using firewalls to divide network segments, detecting and preventing computer attacks to prevent DDoS attacks and similar attacks, and preventing malicious software penetration through measures such as anti-virus protection. The document also proposes the improvement of documents covering areas such as information security review, personnel management, security operations, and standard privacy policies.

4) The Digital Economy Plan of the Russian Federation

On July 28, 2017, Russia officially approved Document No. 1632, The Russian Federation Digital Economy Plan, which includes a roadmap for the future. The goal and task before 2024 is determined within the framework of five basic directions for the development of digital economy, including standardized management, talent and education, cultivating R&D capabilities and technical reserves, information infrastructure, and information security. The plan clarifies the tasks of each stage of Russia's 5G construction.

(3) Ushering in the 5G Commercial Era at the End of July 2020

At the end of July, Russia's largest telecom operator, MTS, obtained a license to provide 5G communication standard services with frequencies of 24.25–24.65 GHz in 83 regions of Russia. MTS became the first in Russia to obtain a 5G license, officially announcing the beginning of the 5G commercial era in Russia. The license will expire in July 2025. MTS said in a statement that the first target groups of 5G network services have been locked, mainly including commercial users and large manufacturers. MTS will soon launch solutions for industrial enterprises.

(4) Influence from the United States

Russia's position has always been clear and firm, and it's no different with 5G. As early as June 2019, Huawei signed a cooperation agreement with Russia's largest telecommunications company MTS, which included the joint development of 5G technology and the trial of 5G networks in 2019 and 2020. Foreign Minister Lavrov announced on August 23 that Russia was ready to cooperate with China and Huawei on 5G technology, instead of following the United States. He emphasized: "We don't have the habits and traditions [that the United States has]." On the contrary, Russia is interested in working with other countries, "co-creating and introducing modern technology into everyday life."

3.2 Examples of "Good Law" and Analysis of Core Clauses

Although some countries have formulated 5G development plans and related standards, they have not implemented an access system for equipment manufacturers. From the current regulations, some countries regulate equipment security from a technical perspective.

(1) Germany

The new version of the telecommunications network security requirements catalogue requires that, "It is necessary to ensure that the security of networks and services, and personal data will not be compromised due to reliance on third parties." In principle, network operators must be responsible for the review of suppliers' reliability, credibility, and quality. During operation, network security should be ensured through continuous security monitoring and other protective precautions. According to this catalogue, companies should pledge to ensure that confidential customer information will not be "sent overseas or notified to foreign agencies in Germany voluntarily or under the instigation of a third party." Violation of the statement will be punished as breach of contract. The catalogue pointed out that when planning and building 5G networks, key networks and system components from different manufacturers should be used to avoid "monocultures".

(2) Spain

Spain's management of telecommunications service providers focuses on the technical level, protecting user rights and ensuring that personal privacy will not be compromised due to technological development. The Information Society and E-Commerce Services Law stipulates that telecommunications service providers are obliged to inform customers of the technical means to protect information security (such as anti-virus, anti-spyware, mail filters, etc.), and at the same time transparently filter certain content and the specific tool of certain

services.

Spain uses technical capabilities as a measure for 5G suppliers, and then has imposed further security requirements. Thus, suppliers will not be selected based on their country of origin.

3.3 Examples of "Bad Law" and Analysis of Core Clauses

By comparing the security legislation of various countries, we see that some have introduced legislation with a discriminatory nature, deliberately excluding some manufacturers, and breaking a fair competition market at government level. Specifically, certain regulations can be divided into two categories. The first category are those establish a non-technical threshold on the grounds of national security, which is typically based on the home country of the equipment manufacturer.

(1) United Kingdom

The 2020 National Security Council meeting of the British government requires the National Cyber Security Centre (NCSC) to issue guidance to British telecom operators on high-risk vendors (HRV), which encompasses the exclusion of HRVs from core functions (i.e., sensitive parts of the network with high security requirements) of the national infrastructure; excluding HRVs from sensitive locations, such as military bases; limiting an HRV's participation to only in the peripheral part of the network and no more than 35%.

The definition of HRV established by NCSC includes the following standards:[51]

a. The vendor's strategic position/scale in the UK network;

b. The vendor's strategic position/scale in other telecoms networks, in particular if the vendor is new to the UK market;

c. The quality and transparency of the vendor's engineering practices and cybersecurity controls;

d. The past behavior and practices of the vendor;

e. The vendor's resilience both in technical terms and in relation to the continuity of supply to UK operators;

f. A number of considerations relating to the ownership and operating location of the vendor, including:

i. The influence which the domestic state apparatus can exert on the vendor (both formal and informal);

ii. Whether the relevant domestic state and associated actors possess an offensive cyber capability that might be used to target UK interests;

iii. Whether a significant component of its business operation is subject to domestic security laws which allow for external direction in a manner that conflicts with UK law.

Observing the laws issued by relevant institutions in the UK, we see that in addition to considering suppliers in terms of their size, security control quality, and past behavior, the

[51] *NCSC advice on the use of equipment from high risk vendors in UK telecoms networks*, https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

NCSC has also issued non-technical territorial politicization standards. Security is also not conducive to full market competition, and the standards may eventually become barriers and weapons for other vendors to form monopolies. In the long run, it may increase the cost of 5G deployment and reduce the country's competitiveness in 5G.

The second category of regulations is to grant government equipment security audit authority through legislation, but the government does not publish security standards, and impedes some equipment vendors through opaque setting.

(2) Estonia

The Estonian government passed the newly revised Electronic Communications Act in 2020. In addition to higher requirements for personal data, it added a security review clause to Article 87. It states that in order to guarantee national security, the Government of the Republic (of Estonia) may impose an obligation on communications undertakings to provide information on the hardware and software used in the communications network. The notification obligation and the notification procedure shall be established and the authority which must be notified shall be designated by a regulation of the Government of the Republic (of Estonia).[52] This law authorizes the government to exclude some communication equipment vendors. In addition, the Prime Minister of Estonia met with US Vice President Pence at the end of 2019, and the two reached an agreement on 5G, which amounted to a "Huawei Law".

Raul Rikk, Director of Estonian Cyber Security Policy, said: "Since we do not always control the technology, we have to make a fundamental decision as to whether or not we trust the manufacturer. This is precisely because the administrative capacity to accurately control each technological component is limited for any country. Simply by reading our foreign intelligence agency's annual report, we know that Chinese technology, for example, is clearly at higher risk."[53]

The Estonian government's security scoring mechanism only involves the government in decision-making and evaluation criteria, and the process is not transparent. This is precisely where relevant legislation may be used to suppress companies in specific countries. The current public standards of the Estonian government include whether it is a listed company and whether it has joined the European Union. These standards are relatively unrelated to security and cannot meet the original goal of the security review.

(3) Poland

The Polish government has not announced the access standards for 5G equipment either, but from the political environment and the country's prime minister's statement, it will likely impose restrictions on specific vendors in the future. Relevant legislation and statements from the Polish government show a number of possibilities:

a. The US-Poland joint statement implies that Poland will be affected by US decision-making in the long term in the use and selection of 5G equipment;

b. Poland's 5G strategy and cybersecurity legislation are trending towards a more stringent replacement of 5G equipment, and Poland's self-positioning as a European 5G technology leader has intensified this trend;

c. There's still the possibility of the Polish government using Huawei equipment. The main

[52] *Electronic Communications Act*, https://www.riigiteataja.ee/en/eli/ee/520052016001/

[53] *Ministry drafts bill aimed at curbing Chinese 5G tech*, https://news.err.ee/1117398/ministry-drafts-bill-aimed-at-curbing-chinese-5g-tech

driving force for the sound development of the relationship between the Polish government and Huawei is the mobile operators such as Play.

3.4 Analysis of the Difference Between "Good" and "Bad"

After sorting out the 5G legislation of various key countries, we further refine the definition process adopted in the "Policies and Regulations-Access Standard Evaluation Quadrant". We make judgments on the status quo of each country and list the potential positive and negative effects caused by legislation according to the corresponding circumstances.

In summary, we believe that the differences between "good" and "bad" law can be summarized into three aspects: transparency, perfection, and objectivity. It is worth noting that these three indicators are independent of each other and require a comprehensive evaluation. Even if a country performs well in one area, it does not mean that it will be deemed "good".

(1) Transparency

Transparency is the most basic condition for operators in selecting equipment suppliers. Legislators should disclose the access criteria as much as possible so that operators have laws and evidence to follow to avoid delays during the initial 5G deployment due to uncertain policies. A lack of transparency leads to ambiguity, and may ultimately result in costs to both operators and equipment suppliers. Outside the EU, the problems caused by transparency have already emerged. Canada is the only country in the Five Eyes Alliance that has not formally excluded Huawei from the construction of 5G networks. However, the government has delayed in making a formal decision to give telecom companies a fear of cooperating with Huawei. India has also excluded Huawei from 5G equipment. The relevant authorities have clearly instructed local telecom service providers to avoid using Chinese equipment in future investments such as 5G, but Indian officials will not issue a formal ban. Huawei is one of India's three major telecom equipment suppliers and has contracts with telecom companies such as Bharti Airtel, Vodafone, and BSNL. Barring Huawei equipment is bound to bring losses to these operators.

As far as transparency is concerned, the UK's approach is worth learning from. Although the UK government's access standards have discriminatory indicators, relevant departments have disclosed specific standards on how to define high-risk vendors. In contrast, although some countries have used legislative means to clarify that the government has the right to exclude 5G vendors, they have not announced the specific criteria for exclusion, which actually brings hidden dangers to operators and 5G vendors in terms of transparency, which is not conducive to the rapid deployment of 5G.

(2) Perfection

Ensuring security is the original intention of countries in formulating 5G legislation. Therefore, in addition to access standards, countries should use specific 5G security standards as the main means to improve 5G security. 5G standard legislation can be very extensive by covering the use of frequency bands, the specifications of facilities, and how to prevent and hold accountable 5G security incidents before and after. Targeted laws and regulations are an important means of information security and network security control. For example, through amendments to existing laws or separate legislation to focus on combating cybercrime, through setting certification standards, trusted parameters, additional technical requirements, and other standard equipment deployment.

Objectively speaking, any communication protocol may have vulnerabilities. In the past,

GSM networks, 3G, and 4G networks all had serious vulnerabilities. Therefore, singling out vendors in and of itself cannot fundamentally rule out possible future security risks. At this point, Germany revised the IT Security Catalogue specifically for 5G, and proposed new security standards and responsibility requirements. However, most countries have not issued specific 5G standards, and the 5G security system has not been perfected.

(3) Objectivity

If a government has issued specific access requirements, objectivity becomes the main criterion for judging good laws from bad ones. Some countries set non-technical thresholds for foreign equipment providers on the grounds of "national security", but they actually put subjective factors such as political considerations before objective security standards. Security standards with strong subjective factors are not conducive to the fair competition of various manufacturers in 5G. They will hinder the healthy development of the market and ultimately damage the 5G leadership of the country. For example, the British government included country of origin in its definition standards, and in fact established an ideological threshold, deliberately excluding Chinese manufacturers.

What is worrying is that since the beginning of the Sino-US trade tensions, the United States has targeted several Chinese high-tech enterprises, with Huawei bearing the brunt. As mentioned in Section 3.2 of this report, the United States, through imposing sanctions and lobbying, is affecting the policies of some European countries for 5G equipment access. Among them, some countries such as the United Kingdom and Estonia have changed their original policies, while others are shifting to a wait-and-see approach.

We believe that objectivity should be the most important criterion in the technical review process. The government should increase transparency and perfection, while emphasizing objective standards at the legislative level, so as to avoid including irrelevant subjectivity in the 5G construction, while avoiding external factors and pressure, typically coming from the United States.

4.Conclusion

As a new yet crucial topic, cyberspace poses a multifaceted challenge to national governance at the cognitive level. The cooperation of significant powers in cyberspace not only faces differences of interests but also more profound dilemmas. As a critical technology in the current intelligent era, 5G communication technology is a hotspot in international technological competition.

The global pandemic is still active, economic globalization is facing a countercurrent, and protectionism and unilateralism prevail in some countries. The United States began lobbying the European Union in mid-2018, trying to use its political power to force Europe into accepting a certain stance on Huawei. From this, one of the essential characteristics of the current European countries' information industry is that it increasingly discriminates against Chinese companies and sets up non-tariff barriers.

This report makes the following recommendations based on existing research.

Firstly, respect the inherent power of globalization and the objective laws of market development, and create and maintain a fair and objective economic and technological environment.

Countries should be deeply aware that singling out countries or manufacturers cannot resolve network security concerns, nor lead to security. They will only destroy the global value chain and isolate the country from better technology applications. Taking sides will widen differences and deepen contradictions, making governance cooperation between countries inefficient or ineffective. It would be helpful to not retire equipment and technology manufacturers in individual countries directly or in disguise based on country of origin.

Secondly, get rid of the single-dimensional security mindset that existed during the Cold War, eliminate false perceptions, build mutual trust, and adhere to open cooperation and security.

By observing the *Policies and Regulations – Access Standard Evaluation Quadrant*, we can see that many countries are still in the exploratory stage of formulating 5G security standards, and the accessibility standards are not yet clear. From the perspective of ensuring 5G security and the healthy development of the market, countries should first ensure that the standards are transparent, and then adopt a reasonable and multi-party discussion to take out political and other non-technical factors into the security measurement standards.

For most countries' strategic requirements, geopolitics is no longer dominated by conflicts and competition, while cooperative governance and shared security have become the smarter choice. In the long run, if Europe, with autonomy in decision-maker, cooperates with China by discounting "values-based diplomacy", realism, and confrontation, then both sides can pool their efforts to avoid systemic security risks. China-EU cooperation can improve the efficiency of regional security governance and global governance capabilities.

Lastly, ICT buyers, operators, and vendors should jointly implement assurance, transparency, and accountability measures to reduce the negative impact of technological nationalism. In 2020, the EastWest Institute's report *Weathering TechNationalism: A Security and Trustworthiness Framework to Manage Cyber Supply Chain Risk* defined TechNationalism as "direct or indirect measures that favor ICT products and services sold by companies headquartered domestically or in allied States against those headquartered in states seen as

competitors or adversaries".[54]

The report believes that *"legitimate national security concerns may justify strict, targeted measures based on accurate threat assessments. Nevertheless, the measures some governments are utilizing to restrain or control foreign ICT can produce unintended effects with negative implications and manifest in many ways. First, bans can motivate technology companies in one country to 'design out' key technologies supplied by companies headquartered elsewhere. Furthermore, innovation in industry sectors accustomed to competition may suffer in the long term; the reduced number of suppliers of goods and services is likely to result in less competition and higher prices. Additionally, there can be strict requirements based on domestic standards, costly technical conformance, and domestic ownership requirements. Finally, investment restrictions reduce foreign capital inflow in emerging domestic industries."*

Therefore, the report proposes that ICT buyers, operators, and vendors should jointly implement an "Assurance, Transparency, and Accountability Framework" to mitigate risks and respond to joint responsibilities in the global ICT supply chain as well as to reduce possible security risks through transparent measures, thereby reducing the negative impact of nationalistic technological measures.

In summary, our report finds that 5G is essential for the evolution of this generation of information and communication technology. Its rapid development will have an all-encompassing and in-depth impact on the development of politics, economy, culture, society, and other areas globally. Furthermore, it will reconstruct the global innovation landscape and reshape the structure of the economy. Therefore, all countries have typical demands to promote the digital economy's development and respond to security risks and challenges. 5G network security risks should be viewed objectively, and global standards and rules for 5G security should be discussed and formulated on a multilateral platform where all parties can participate.

In order to effectively respond to global challenges, all parties should break through the limitations of the single-dimensional security mindset that existed during the Cold War, eliminate false perceptions, establish mutual trust, adhere to the concept of open and cooperative security, and establish corresponding cooperation and governance mechanisms in order to build amicable relations between great powers over cyberspace and maintain its stability, peace, and development.

Cooperation with Europe in cyberspace has multiple positive strategic implications for China. The systemic impact of the union between Asia and Europe and Sino-European cooperation is of profound theoretical and practical importance. For example, it can alleviate the peripheral security strategy pressure brought on by the US hegemony. Non-traditional security, multi-dimensional security, and cooperative security constitute the theoretical implications of the new security concept. In the field of policy, China and the EU will respond to the needs of the times and realize that cooperative security, as the core of the new security concept, has gradually become the clear choice to deal with globalization and the issues that come with it.

[54] *Weathering TechNationalism: A Security and Trustworthiness Framework to Manage Cyber Supply Chain Risk*, EastWest Institute, https://www.eastwest.ngo/sites/default/files/ideas-files/weathering-technationalism.pdf.

编辑部：**复旦大学发展研究院**
EDITORIAL DEPARTMENT: **FUDAN DEVELOPMENT INSTITUTE**

Address: Think Tank Building, Fudan University,
No. 220 Handan Road, Shanghai, China
Post code: 200433
Tel: 86-21-55670203
Email: fdifudan@fudan.edu.cn
Website: http://fddi.fudan.edu.cn