The Research on Cybersecurity Risks in 5G network: Perspectives on Global strategy

The Research on Cybersecurity Risks in 5G network: Perspectives on Global strategy

I. The characteristics of 5G and cybersecurity threats

Compared to 4G, 5G adopts several new designs on the network architecture, such as software-defined networking (SDN), a baseband unit (BBU), logical disjunction, network function virtualization (NFV), and multi-access edge computing (MEC), to provide users with high-speed, low-latency and other quality services, as well as flexibility and expansibility to accommodate more emerging applications.

According to the three key usage scenarios (see Figure 1) defined by the International Telecommunication Union (ITU), enhanced mobile broadband access (eMBB) provides high-volume mobile broadband services such as AR/VR or ultra-high-definition video. Massive machine type communication (mMTC) provides large-scale IoT services. Ultra-reliability and low latency communication (uRLLC) can be used for services that require low-latency and high-reliability connections, including unmanned driving and industrial automation.

However, with 5G's open, flexible and extensible design, as well as its coexistence with other 4G and 3G systems in the early stage of commercial operation, the cybersecurity threats facing 5G networks are more severe and diverse than the past mobile phone generations. At present, the known 5G cybersecurity threats mainly come from network functional components and connection interfaces among components, including the terminal device, access network, air interface, cloud virtualization, multi-access edge computing rental, core network, back-end/backbone network, roaming and external services, and so on.

Source: ITU

Figure 1 Three key 5G scenarios by the ITU

II. Cybersecurity strategy development in major countries

5G is not only one of the critical infrastructures, but also an important foundation for pursuing a digital nation, digital economy, the industrial 4.0, and for promoting industrial transformation for upgrading. However, different scenarios require different cybersecurity protection levels, which poses great challenges to both mobile network operators and service providers.

Therefore, the construction of favorable environment for 5G development, the promotion of relevant applications and the development of innovative services and so on, have become the priority of governance in the countries around the world.

1. European Union (EU)

Then European Commission President Jean-Claude Juncker noted in 2017 that "Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks…Cyber-attacks know no borders and no one is immune," indicating the EU's high priority in the cybersecurity field.

The "Digital Single Market," an important EU policy, lays the foundation for digital economy based on "cybersecurity, trust and privacy." In response to the loss of billions of euros a year in cyber attacks, the EU has taken a series of measures to safeguard and advance the development of the Digital Single Market. For the purposes of this strategy, the European Commission in 2018 came up with the policy of Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,[1]with the aim of improving the level of cyber security, cyber resilience and trust in the EU, and in June 2019 passed the Cybersecurity Act [2] with two highlights described as follows:

(1) Strengthen the authority of the European Union Agency for Network and Information Security (ENISA)(see Figure 2), increase the allocation of human and financial resources to ENISA, as well as the preparation for the work items related to the cybersecurity industry, and reinforce cyber security support for EU member states.

(2) Establish the EU cybersecurity certification framework. [3]

In the European Union, where different cybersecurity certification schemes already exist, the absence of a common certification regime would increase the risk of fragmentation of the single market. For this reason, a set of technical requirements, standards and procedures are provided under this framework to assess whether information/communication products, services and processes are in compliance with security requirements.

The certification program includes product and service categories, information/communication security requirements (e.g. reference standards or technical specifications), types of assessment (e.g. self-assessment or third-party assessment), levels of security, and so on. All member states agree that certification not only facilitate cross-border business transactions, but also enable consumers to better understand the security of products and services.

Source: Compiled from the ENISA websit

Figure 2 ENISA organization and authority strengthening

2. the United States (U.S.)

In consideration of cyber security affairs in the country, the US Department of Homeland Security (DHS) in May 2018 unveiled the "Cybersecurity Strategy,"[4] which focused on the objectives and priorities of the U.S. government in future cybersecurity protection, identifying and managing national cybersecurity risks with the overall risk management approach, and addressing security threats to the country, critical

infrastructures and private enterprises, as well as preventing cybercrimes.

Then the White House in September 2018 released the National Cyber Strategy of the United States of America, [5] based on the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [6] issued in May 2017, stating the strategy and position of the United States against the threat of cyber- attacks. The strategic goal aimed to, by safeguarding cybersecurity, protect the American people, the homeland, and the American way of life, to build a secure digital economic environment, to promote American prosperity, and strengthen cooperation with partners to deter malicious cyber attackers, so as to maintain peace and security, and continue to expand U.S. influence.

The department in July 2019 published the Digital Modernization Strategy [7] to announce its national defense strategy in the digital environment, including the use of cybersecurity, AI, cloud computing, blockchain and other technologies in information security protection to create a more secure, coordinated and efficient platform and improve the security of intelligence transmission and processing.

3. Canada

Public Safety Canada in June 2018 released the National Cyber Security Strategy, [8] with the vision of a sustainable, robust cybersecurity environment, innovation and prosperity. Through international cooperation and a domestic public-private partnership, the department has been working on three goals: 1. cyber security and resilience (to reduce cybercrime and ensure Internet privacy; 2. Internet innovation (to create a friendly environment for the development of cybersecurity startups); 3. government leadership and cooperation (to transfer government-owned cybersecurity knowledge to the private sector and set up a cybersecurity governance framework).

The Canadian government also attaches great importance to critical infrastructure. In May 2018, the National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure [9] was unveiled to facilitate information sharing between public and private partners through sharing and protecting intelligence, and implementing a full risk management approach. Moreover, Public Safety Canada in April 2019 issued a report called Enhancing Canada’s Critical Infrastructure Resilience to Insider Risk, which provided guidelines and suggestions for action on internal risks in critical infrastructure organizations.[10]

4. Singapore

The government of Singapore in 2018 promulgated the Cybersecurity Act, [11] which aimed to fulfill the vision of a Smart Nation by enacting and putting into effect cybersecurity regulations to achieve the goal of a resilient infrastructure and a more secure cyberspace, and to strengthen the protection of critical information infrastructure against cyber-attacks. The Cyber Security Agency of Singapore (CSA) was given the authority to prevent and respond to cybersecurity threats, and to set up a system for sharing security information, as well as a light-touch licensing system for cybersecurity service providers.[12]

The Government of Singapore has appointed a Commissioner of Cybersecurity responsible for promoting domestic cybersecurity policy. To safeguard Singaporeans from cybersecurity threats, [13] the government particularly laid down cybersecurity threat or incident response provisions in Chapter 4 of the Cybersecurity Act to empower the Commissioner of Cybersecurity to investigate cybersecurity threats and incidents, such as requiring the parties to the incidents to present statements in person or in writing, producing documents or provide information and so on.[14]

5. Australia

The Australian government in 2016 proposed a four-year "Australia's Cyber Security Strategy,"[15] which was expected to invest more than 230 million Australian dollars to strengthen Australia's cyber security capability and complete the following five aspects: national cyber partnership, strong cyber defenses, global responsibility and influence, growth and innovation, and a cyber smart nation.

As for the global responsibility and influence, the Australian government in 2017 announced the "Australia's International Cyber Engagement Strategy."[16] which aims to strengthen digital trade, to improve cybersecurity and to response to cybercrime through international cooperation; encourage innovative cybersecurity solutions; provide security advice and best practices, such as Essential Eight strategies[17] to mitigate cyber-attacks; establish the Pacific Cyber Security Operational Network (PaCSON) [18] with neighboring countries to develop regional cybersecurity capabilities; and advance the development of Australia's cybersecurity industry, nurture startups and attract foreign investment.

III. Cybersecurity strategy to promote 5G in Taiwan

Since President Tsai Ing-wen took office in 2016, she declared that cybersecurity is directly linked to national security. In 2017, the Department of Cyber Security (DCS) under the Executive Yuan issued "National Cybersecurity Development Plan (2017-2020)," and in 2018 the "Cybersecurity Industry Development Action Plan (2018-2025)," in order to enhance the independence of Taiwan's cybersecurity industry, consolidate the nation’s cybersecurity defense line, improve its innovative thinking of cyber security, and further promote it to the international market.

To develop a favorable environment to promote 5G, the Executive Yuan on May 10, 2019 approved the “Taiwan 5G Action Plan (2019-2022),” [19] with a total investment about NT$20.466 billion over a four-year period. The plan aims to build a 5G application and industrial innovation environment, and reshape Taiwan's mobile communication industry ecosystem, with its content planned around five themes, including "promoting 5G vertical application field demonstration", "building 5G innovation and application development environment," "completing 5G technology core and cybersecurity protection capabilities," "planning to release 5G frequency spectrums in line with overall interests" and "adjusting laws and regulations to create favorable environment for 5G development," and to promote industrial upgrading and transformation, as well as create the next wave of economic prosperity in Taiwan.

Secure, robust and reliable 5G systems are sufficient and requisite conditions for building an innovation ecosystem in digital countries. The third theme of the "Taiwan 5G Action Plan" is to "complete 5G technology core and cybersecurity protection capabilities," which is intended to advance the integration of applied science and technology by establishing advantageous core technologies, set up a 5G technology and test platform, and increase the market competitiveness of 5G industry, while drafting the overall national policies on 5G

cybersecurity, building the cybersecurity protection mechanism of 5G homemade products, strengthening 5G critical infrastructure and operational cybersecurity protection capabilities, and promoting domestic suppliers to enter the international 5G reliable supply chain.

In terms of strengthening 5G critical infrastructure and operational cybersecurity protection capacities, the NCC has planned a four-year (2019-2022) "5G Network Cybersecurity Protection and Related Regulations Preparation Plan." In coordination with a 5G license issue in 2020, the agency in 2019 added/amended the 5G cybersecurity provisions of the Regulations for Administration of Mobile Broadband Businesses, making it mandatory for the winning bidder of the 5G frequency spectrum to incorporate the cybersecurity protection concept into the system design for system construction.

Upon commercial operation of 5G, the NCC will audit from time to time the implementation of the cybersecurity maintenance plan by telecom operators, so as to ensure and reinforce the cybersecurity protection system of Taiwan's 5G telecom network, and create an opportunity for the development of 5G homemade products with cybersecurity protection capability. In addition, the NCC will also face up to the fact that 5G technology standards continue to evolve, and the operators have different construction schedules and heterogeneous mobile networks coexist. Therefore, relevant regulations will continue to be completed from 2020 to 2022, and examples will be verified through cybersecurity function testing laboratories to ensure that cybersecurity protection functions of 5G networks keep pace with the times.

IV. Conclusion and Suggestion

As for emerging technologies, countries around the world are actively evaluating and constructing 5G systems and services. Taiwan boasts excellent industrial advantages in terms of semiconductors, ICT software and hardware, and high-quality talents, and thus makes a foundation for developing 5G. Furthermore, going with the importance of cybersecurity, it is necessary to pay more attention to planning and developing 5G cybersecurity technology.

It is clear that the development of cybersecurity is both a challenge and an opportunity for Taiwan. In order to implement the national policy objectives of "cybersecurity is national security" as well as "innovative economic development programs for a digital nation," and to response to the scientific and technological progress, and the demand for cybersecurity, key development direction is proposed to expedite the establishment of 5G cybersecurity protection.

Reference:

[1]Resilience, Deterrence and Defence: Building strong cybersecurity in Europe, European Commission, https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe

[2]The draft Regulation of The European Parliament And of The Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation(EU)526/2013, and on Information and Communication Technology cybersecurity certification("Cybersecurity Act") was published in September 2017 to expand the rights and obligations of ENISA, which would make ENISA the EU's cybersecurity and information competent authority and the authority for critical infrastructure (information) facilities after the passage of the Act.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

[3]The EU cybersecurity certification framework, European Commission, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

[4]Cybersecurity Strategy(2018), DHS, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

[5]National Cyber Strategy of the United States of America(2018), The White House, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[6]THE WHITE HOUSE, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, The White House, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[7]DoD Digital Modernization Strategy, DoD, https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF

[8]National Cybersecurity Strategy, Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

[9]National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure, Public Safety Canada, Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2018-20/index-en.aspx#a02

The action plan is a three-year program under Canada's2010 National Strategy for Critical Infrastructure (National Strategy) starting in 2010 for all phases.

[10]Enhancing Canada’s Critical Infrastructure Resilience to Insider Risk, Public Safety Canada, Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/index-en.aspx

[11]Cybersecurity Act 2018, Singapore Statutes Online, https://sso.agc.gov.sg/Acts-Supp/9-2018/

[12]Cybersecurity Act, CSA, https://www.csa.gov.sg/legislation/cybersecurity-act

[13]*Id.*

[14]Cybersecurity Act Explanatory Statement, https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/cybersecurity%20act%20-%20explanatory%20statement.pdf

[15]Australia’s Cybersecurity Strategy, https://cybersecuritystrategy.homeaffairs.gov.au/

What is the Government doing in cybersecurity, Ministers for the Department of Industry, Innovation and Science, https://www.industry.gov.au/data-and-publications/australias-tech-future/cyber-security/what-is-the-government-doing-in-cyber-security

[16]Australia’s International Cyber Engagement Strategy, Department of Foreign Affairs and

Trade,https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf
[17]Essential Eight Explained, ACSC, https://www.cyber.gov.au/publications/essential-eight-explained
[18]Pacific Cybersecurity Operational Network(PaCSON), https://dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/Pages/pacific-cyber-security-operational-network-pacson.aspx
Or Strengthening cybersecurity across the Pacific, ACSC, https://www.cyber.gov.au/news/pacific-islands
PaCSON is comprised of 15 members, including Australia, Fiji, Marshall Islands, New Zealand, Papua New Guinea, Samoa, and Solomon Islands.
[19]Taiwan 5G Action Plan, Executive Yuan,https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/087b4ed8-8c79-49f2-90c3-6fb22d740488

Links

- Resilience, Deterrence and Defence: Building strong cybersecurity in Europe
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)
- The EU cybersecurity certification framework
- Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- National Cybersecurity Strategy
- National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure
- Enhancing Canada's Critical Infrastructure Resilience to Insider Risk
- Cybersecurity Act 2018
- Cybersecurity Act
- Australia's Cybersecurity Strategy
- What is the Government doing in cybersecurity
- Essential Eight Explained
- Pacific Cybersecurity Operational Network(PaCSON)
- Strengthening cyber security across the Pacific
- Taiwan 5G Action Plan

Download

- Cybersecurity Strategy(2018) [pdf]
- National Cyber Strategy of the United States of America(2018) [pdf]
- DoD Digital Modernization Strategy [PDF]
- Cybersecurity Act Explanatory Statement [pdf]
- Australia's International Cyber Engagement Strategy [pdf]

Juan, Yun-Chien
Associate Legal Researcher

Release : 2020/06