BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 6 • N° 23 • JUNE 2020

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

LOGIC AND KEY POINTS OF CHINA'S CYBERSECURITY REVIEW MEASURES

by Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China.
Edited by Vagelis Papakonstantinou, Brussels Privacy Hub

China's Cybersecurity Review Measures ("Review Measures") were released on April 13, 2020 and will take effect on June 1, 2020. The Review Measures will replace the Network Product and Service Security Review Measures (Trial) that have been in effect since 2017. From the initial trial to the final version, the Review Measures have been gradually condensed and refined over a three-year period of practice and exploration. This document uses 5G security as an example to analyze the logic and key points of the Review Measures.

Key Words: China Cybersecurity Act, China Cybersecurity Review Measures, 5G security

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.

Disclaimer

Introduction

China's Cybersecurity Review Measures ("Review Measures") were released on April 13, 2020 and will take effect on June 1, 2020. The Review Measures will replace the Network Product and Service Security Review Measures (Trial) that have been in effect since 2017. From the initial trial to the final version, the Review Measures have been gradually condensed and refined over a three-year period of practice and exploration. This document uses 5G security as an example to analyze the logic and key points of the Review Measures.

1. China's Existing 5G Security Legal Framework

At present, China's telecommunications and cyberspace authorities have not proposed any regulatory documents specific to 5G security. In the ***5G Security Report*** released in February 2020, the China Academy of Information and Communications Technology (CAICT), under the Ministry of Industry and Information Technology (MIIT), mentioned, "To properly handle 5G security issues, we can build on the existing 4G security management framework and technical support measures and take targeted measures to address new security risks and uncertainties." This means that the Cybersecurity Law and the Telecommunications Regulations jointly form China's 5G security legal framework until China implements specific 5G legislation. In this section, we analyze China's existing 5G security legal framework with regard to major stakeholders in the 5G ecosystem.

For mobile network operators, "Chapter III: Network Operations Security" of the Cybersecurity Law and "Chapter V: Telecommunications Security" of the Telecommunications Regulations both apply. The Cybersecurity Law will almost certainly recognize 5G mobile networks as Critical Information Infrastructure (CII), meaning that CII operators shall assume specific enhanced security obligations in addition to the security obligations of general network operators.

In the Telecommunications Regulations, there are no provisions specific to suppliers of 5G mobile network operators, manufacturers of network devices, and related service providers. The Cybersecurity Law has the following general requirements:

Security of products or services	Article 22: Providers of network products and services must not install malware, and shall promptly adopt remedial measures when security defects are discovered, provide security maintenance as agreed, explicitly notify users of functions that collect user information, and more.
	Article 23: Critical network equipment and specialized cybersecurity products shall follow compulsory certification and inspection requirements.
	Article 36: CII operators purchasing network products and services shall sign non-disclosure agreements with providers according to regulations, clarifying duties and responsibilities for security and confidentiality.

Security impact of products or services on CII	Article 35: CII operators purchasing network products and services that might influence national security shall undergo security clearance organized by the national network information department and relevant departments of the State Council. **Note: The Review Measures refine the provisions of Article 35 of the Cybersecurity Law.**

Other service and content providers that have 5G network access may also be general network operators or CII operators, and therefore shall comply with the relevant provisions of the Cybersecurity Law and the Telecommunications Regulations as well.

2. Basic Logic and Key Points of the Review Measures

Given the details provided in the previous section, we can conclude that the Review Measures tend to address the potential security issues that may arise from the use of products or services in CII. In other words, cybersecurity review is required because specific CII operators (i.e., 5G mobile network operators) may bring vulnerabilities to 5G networks due to their purchase of specific network products and services, rather than inherent security issues in products or services. These inherent security issues are addressed in Articles 22, 23, and 36 of the Cybersecurity Law and by relevant supporting systems. This is key to understanding the Review Measures, and with this basic logic, we are better able to understand all aspects of the review system established by the Review Measures.

2.1 The review objects are clear

The Review Measures stipulate that security review aims to "ensure a secure supply chain for critical information infrastructure and safeguard national security", focusing on the risks that products and services may pose to CII in terms of supply chain security.

This clearly means that the specific products and services purchased by CII operators are defined as review objects pursuant to the Review Measures. The Review Measures also specify the scope of products and services subject to review. Article 20 is clear in this regard: "Network products and services mentioned in these Measures primarily refer to core network equipment, high-performance computers and servers, large-capacity storage devices, large-scale databases and application software, cybersecurity equipment, cloud computing services, and other network products and services that have a significant impact on the security of CII." With regard to 5G suppliers, the Review Measures stipulate the review on their "compliance with applicable Chinese national laws, administrative regulations, and department rules". In summary, the scope of objects subject to review under the Review Measures is clear, targeting specific products and services primarily, supplemented by suppliers. The review of suppliers shall not be independent of the specific products or services that they provide. Overall, China does not proactively conduct independent review or risk assessment targeting a specific supplier.

2.2 The factors to assess are specific.

The core of the Review Measures is to examine specific products or services and specific application sce-

narios. This reflects an advanced perception of security, namely, cybersecurity is a relative rather than an absolute concept. Similarly, the security of products and services is relative. Whether a product or service is secure largely depends on multiple factors, such as who is using it, how and why it is used, and the reliability of supply channels. As a result, there is no absolute and constant benchmark for measuring security. Therefore, the cybersecurity review stipulated in the Review Measures focuses on whether the procurement and use of specific products and services will bring the following:

The risk that the use of products and services could allow the illegal control of, interference with, or destruction of CII, as well as the risk of theft, leakage, or damage of important data (Paragraph 1 of Article 9) The harm to CII business continuity caused by disruptions in product and service supply (Paragraph 2 of Article 9)

Paragraph 3 of Article 9 stipulates the review on "the security, openness, transparency, and diversity of sources of products and services". We can interpret the rough meaning of this as follows: Security refers to whether products and services have risks of being intruded, damaged, destructed, tampered with, or manipulated. Openness refers to the compatibility and interoperability of products and services. Transparency refers to whether network operation personnel can understand, adjust, and control the working principles and mechanisms of products and services. A diversity of sources shows the need to avoid over-dependence.

Paragraph 3 of Article 9 further stipulates the review on "the risk of supply disruptions caused by political, diplomatic, and trade factors". In essence, this is a further review of the factors that may cause supply disruptions. For example, because Microsoft no longer provides security updates for the Windows XP operating system, the party and government organizations' information systems that use this operating system may be exposed to security risks. Another example of this is the export control measures used by the US to control the global supply chain of chips. Such measures can affect whether a specific type of chip purchased for CII can be continuously supplied.

From the above analysis, we can conclude that China does not consider the suppliers' country of origin when assessing risks. Cybersecurity review has always focused on specific products and services, as well as the vulnerabilities that may be introduced by the use of the products or services to specific CII. It therefore goes without saying that cybersecurity review is primarily a technical and objective assessment. In the words of an official at Cyberspace Administration of China replying to media questions about the Review Measures, "Cybersecurity review aims to safeguard national cybersecurity, not to restrict or discriminate against foreign products and services. China has stayed committed to the fundamental national policy of opening-up, and always welcomes foreign products and services to enter the Chinese market."

2.3 The review is initiated by operators.

As stipulated in the Review Measures, the main condition for review is as follows: "Operators that purchase network products and services shall anticipate the potential risks to national security posed by the purchased products and services after they are put into operation. If they affect or may affect national security, a cybersecurity review shall be reported to the Cybersecurity Review Office."

This shows that the entities required to report a cybersecurity review are the CII operators that purchase network products and services. They must also proactively "anticipate the potential risks to national se-

curity posed by the purchased products and services" and determine whether to report a cybersecurity review accordingly. This is one of the legal obligations of the purchaser. Furthermore, the purchaser shall proactively manage its own supply chain risks through legal work. For example, Article 6 stipulates that "operators shall require product and service providers to cooperate with the cybersecurity review through procurement documents or agreements, etc., including a commitment not to exploit the supply of products and services as a convenient way to illegally gain access to user data or illegally control and operate user equipment, or not to cut off product supply or necessary technical support without reasonable grounds".

Because the purchaser selects the specific products and services to be reviewed, we can outline the purchaser's role, while also considering the purchaser's legal obligations mentioned earlier, as defined in the Review Measures — subject of liabilities (compliant with the principle of parity of authority and responsibility). This means that the purchaser shall proactively manage and mitigate supply chain security risks as long as they can.

We can therefore conclude that China's regulatory arrangements greatly respect the risk judgment and business decision-making of 5G network operators based on their own operation scenarios, and avoid any indiscriminate and large-scale government intervention in enterprises' daily purchasing activities. In other words, the cybersecurity review mechanism will be initiated only when operators fail to control the security risks caused by the use of a product or service in a specific scenario.

Such a regulation, in turn, prevents public authorities from proactively intervening in the 5G supply market and assessing supplier risk profiles and diversity of suppliers, thereby preventing the 5G supply market from becoming heavily planned and regulated, which would subsequently lead to the market losing vitality and motivation for innovation.

2.4 Review conclusions are deliberate.

Because the core of the Review Measures is to examine specific products or services and specific application scenarios, the review concludes whether a specific product or service can be used in a specific scenario. In other words, even if a product or service fails to pass one cybersecurity review, it will not necessarily fail another cybersecurity review initiated by different 5G operator. According to this logic, to avoid a product or service being perceived as insecure throughout the market, the review conclusion will be notified to "the operator in writing" (Article 12) in most cases, and will not be disclosed to other operators or society.

This is the case because the specific products or services purchased by CII operators are always the review objects pursuant to the Review Measures. Therefore, even if a product or service fails to pass a review, it does not mean that all CII operators will reject the products or services provided by the supplier. It means that one failure will not result in an overall failure.

Brief Summary

As we have discussed above, China's cybersecurity review does not consider the suppliers' country of origin. In other words, the risk profiles of suppliers are not the starting point for assessing security.

Moreover, China's cybersecurity review assesses the product or service rather than labeling a supplier. The failure of a supplier's product or service in one review only indicates that CII operators should not use this specific product or service in specific scenarios or phases. It does not affect any other products or services offered by this supplier, thereby avoiding any collateral damage.

China's cybersecurity review respects operators' independent decision-making on security, which in turn encourages operators to improve their security levels.

In general, China's cybersecurity review system is designed to not only maintain the diversity of the 5G supply market, but also encourage network operators from different countries to compete with each other and make continuous innovation, thereby driving sustainable development of 5G networks.

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri and Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommunications operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou and Paul de Hert (13 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

N°16 Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an *interim* period of no regulation at all) (June 2019) by Vagelis Papakonstantinou and Paul de Hert (25 pages)

N°17 Data Localisation: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU (September 2019) by Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (31 pages)

N°18 Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination (January 2020) by Dr Monique Mann and Professor Tobias Matzner (18 pages)

N°19 Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment? (February 2020) by Lina Jasmontaite and Paul de Hert (23 pages)

N°20 The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? (March 2020) by Elena Gil González, Paul De Hert & Vagelis Papakonstantinou (31 pages)

N°21 Article 8 ECHR compliant and foreseeable surveillance: the ECtHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law (April 2020) by Paul De Hert & Gianclaudio Malgieri (42 pages)

N°22 The "Ethification" of Privacy and Data Protection Law in the European Union. The Case of Artificial Intelligence (May 2020) by Niels van Dijk and Simone Casiraghi (23 pages)

N°23 Logic and Key Points of China's Cybersecurity Review Measures (June 2020) by Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (9 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.eu