CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Approaches to the Supply Chain Cybersecurity: Taking a More Restrictive Stance Against High-Risk Vendors

Keiko Kono and Samuele De Tomas Colatin

Tallinn 2023

About the authors

Keiko Kono and Samuele De Tomas Colatin are former legal researchers at the Cooperative Cyber Defence Centre of Excellence (CCDCOE) Law branch.

CCDCOE

The NATO CCDCOE is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE is a diverse group of international experts from the military, government, academia and industry, currently representing 39 nations.

The CCDCOE maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations and law.

The Tallinn Manual, prepared at the invitation of the CCDCOE, is the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields allows cybersecurity experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decision-makers from the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring.

The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. NATO-accredited centres of excellence are not part of the NATO Command Structure. www.ccdcoe.org publications@ccdcoe.org

Disclaimer

Table of Contents

Acknowledgements

The authors would like to thank Sungbaek Cho, Cdr Davide Giovannelli, Kadri Kaska, Masayuki Matsuoka, Naoki Nakatani, Pentti Olin, Keishi Ono, Olena Roraff and Kei Tsukada for their valuable comments and suggestions. They would also like to thank Lt Col Ben Valk, a researcher at the CCDCOE Law branch, for his overall review and finalisation of the publication process. Without this support, the paper would not have been published.

Abbreviations

CCDCOE	The NATO Cooperative Cyber Defence Centre of Excellence
CSA	Connected software applications
CSM	Cyber Security Model
CSSH	Cybersecurity Strategic Headquarters
EAR	Export Administration Regulations
ENISA	European Union Agency for Cybersecurity
EO	Executive Order
EU	European Union
FAR	Federal Acquisition Regulations
FCC	Federal Communications Commission
GGE	Groups of Governmental Experts
HRV	High-risk vendor
ICSID	International Centre for Settlement of Investment Disputes
ICT	Information and communications technology
ICTS	Information and communication technology and services
IEEPA	International Emergency Economic Powers Act
JSDF	Japan Self-Defense Forces
METI	Ministry of Economy, Trade and Industry
MIC	Ministry of Internal Affairs and Communications
MOD	Ministry of Defence
MoU	Memorandum of Understanding
NATO	The North Atlantic Treaty Organisation
NCSC	National Cyber Security Centre
NDAA	National Defense Authorization Act
NISC	National center of Incident readiness and Strategy for Cybersecurity
NIST	National Institute of Standards and Technology
OEWG	Open-Ended Working Group
SAQ	Supplier assurance questionnaire
SBOM	Software Bill of Materials
SCO	Shanghai Cooperation Organisation
Traficom	Finnish Transport and Communications Agency
WTO	The World Trade Organisation

Abstract

Supply chain attacks are among the most significant security concerns to nations. There are a variety of options to mitigate supply chain cybersecurity risks, yet none is perfect, especially for state-sponsored cyber threats. This paper focuses on preventative approaches and intends to give an overview of national practices in selected countries: Finland, Japan, the United Kingdom, and the United States.

There are no international legally binding rules or principles in the cybersecurity of the supply chain and a growing number of states perceive the need for national frameworks and mechanisms for ensuring the cybersecurity of the supply chain and globally common rules, as shown in some discussions ongoing at the UN. Western countries have developed frameworks at the regional and national levels based on their commonly shared perception that the supply chain is vulnerable to threats from adversarial foreign countries and that these threats must be effectively addressed by strengthening national regulations.

Despite a lack of binding agreements, all four countries reviewed in this paper have some domestic legislation or documents to regulate the supply chain and safeguard national security and foreign policy interests. Except for Japan, they passed laws addressing various cybersecurity issues. In the defence arena, all but Finland are comprehensive in covering almost all products and services, at least from the publicly available information. Finland's regulations appear more limited in scope as they only focus on 'the most critical parts of the communication network.' The UK and the US are explicit in targeting high-risk vendors such as Huawei and particular countries such as China and Russia (in the case of the US) and strict requirements are imposed on domestic providers to remove these risk vendors from their network systems. Finland and Japan are implicit in this regard. However, all four nations have come to a similar practice by excluding or refraining from acquiring certain products and services made by certain countries.

National practices on the topic of the cybersecurity of the supply chain and the threat perceptions behind these practices vary between countries, including across the EU and NATO making it even more difficult to develop common international rules and standards. However, there is a pressing need to address the threats ahead of actual incidents since no country is exempt from supply chain cyberattacks and further exchange of good practices between countries is recommended in the UN GGE 2021 Report (para. 57 (b)). Transparency, objectivity and impartiality of these national approaches are key to success, as proposed in the UN GGE Report (para. 57 (a)).

1. Introduction

Supply chain attacks are significant security concerns to nations. The European Union Agency for Cybersecurity (ENISA) reported that there were 24 confirmed supply chain attacks between January 2020 and early July 2021 and more than 50% of these attacks were attributed to well-known state-sponsored cybercriminal groups.[1] While analysis of these past cases and attribution is important from a law enforcement perspective, this paper focuses on preventative approaches and intends to give an overview of national practices in Finland, Japan, the United Kingdom, and the United States.

Concern about cyber threats in the supply chain is not new, but a perception as to what constitutes cyber threats to supply chain security may vary by country. There are also a variety of options to mitigate supply chain cybersecurity risks but none of these is perfect, especially for state-sponsored cyber threats. Think of an ICT company headquartered in a state where that company has close ties with authorities and its software products are widely used for critical infrastructure around the globe. Other scenarios may include gaining unauthorised access to a closed network and inserting backdoors to a victim's computer terminal by perpetrators who may not even be in the country. In such cases, it is far from easy to arrest and punish criminals. What the US Congress did to Kaspersky products in 2017 was to remove them from government procurement, even though it was fully certified under the US government-run validation programme. Other countries are taking a similar approach.

With such national security interests in mind, this paper starts with frameworks at the regional level: the US-led Clean Network Initiative for 5G and the EU Toolbox of risk mitigating measures (Chapters 2 and 3). Chapter 4 explores what regulatory measures are in place in these countries and whether the measures are removing particular vendors or countries from the defence arena. To this date, there is no binding international agreement on this matter and only diplomatic negotiations at the UN provide a norm that is distinct from legally binding rules and principles. Chapter 5 confirms what has been agreed upon and what has yet to be agreed upon at the UN. With growing numbers of similar national approaches, more and more countries will become aware of the problem and this will help to shape international agreement. Chapter 6 seeks commonalities of the threat perception and measures in place with a view to looking for more legislative moves at regional and multilateral fora.

This report is written by Keiko Kono overall, and Chapter 3 is written in part by Samuele De Tomas Colatin. Legislative efforts in respective nations and international organisations are ongoing and this paper thus is not conclusive and definitive but a study, hoping to be followed by further analysis in the future.

[1] ENISA, 'Threat Landscape for Supply Chain Attacks,' July 2021, pp. 22 and 25, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks. The report lists APT29, APT41, Thallium APT, UNC2546, Lazarus APT, TA413 and TA428 as the groups behind these supply chain attacks.

2. United States' 'Clean Network' Initiative for 5G

This is the US-led initiative announced by Secretary of State Pompeo on 29 April 2020 to provide a 'clean path for all 5G network traffic coming into all of [US State Department systems…] to keep our critical data and our networks safe from the Chinese Communist Party'.[2] It was later expanded to include a range of variations such as Clear Carrier, Clean Store, Clean Apps, Clean Cloud and Clean Cable in August of the same year.[3] 'Clean', in this context, is removing any equipment produced by untrusted IT vendors such as Huawei and ZTE. According to the archived website of the US Department of State, 60 countries and regions and over 200 telecommunication companies had joined this Alliance by mid-January 2021.[4] The EU and NATO also supported it and many member countries have signed a joint declaration or Memorandum of Understanding (MoU) on 5G security with the US. The list of countries is not available on the website but there is a graphic on transatlantic countries (see Figure 1).[5] It is, however, unclear whether and how the Biden Administration has improved on the previous administration's legacy. In the best-case scenario where all joint declarations and MoUs remain valid, 28 of the 31 NATO Allies and 26 of the 27 EU Members are still on board.[6] It is not yet confirmed which nations in Europe are distancing themselves from the programme,[7] apart from Hungary.[8]

The MoU/joint declaration may not have named China or Chinese companies explicitly, but it clearly indicates concerns over the control of suppliers by a foreign government. The Slovak Republic's Joint Declaration on 5G Security signed on 23 October 2020, for example, provides as follows.

> [Both countries] believe that a rigorous evaluation of suppliers and supply chains should take into account the rule of law; the security environment; ethical supplier practices; and a supplier's compliance with security standards and best practices. Specifically, evaluations should be careful and complete and include especially the following elements:

---

[2] 'Secretary Michael R. Pompeo At a Press Availability: Remarks to the Press,' 29 April 2020, Archived US Department of State website, https://2017-2021.state.gov/secretary-michael-r-pompeo-at-a-press-availability-4/index.html

[3] https://2017-2021.state.gov/the-clean-network/index.html

[4] The archived US Department of State website, 'Under Secretary Keith Krach Remarks on U.S.-Eswatini Clean Network Declaration,' 15 January 2021, https://2017-2021.state.gov/under-secretary-keith-krach-remarks-on-u-s-eswatini-clean-network-declaration/index.html

[5] This graphic is often cited as a material presented by the US State Department. https://www.zdnet.com/article/four-more-european-nations-sign-onto-us-5g-security-agreements/; https://dailynewshungary.com/hungarian-foreign-ministry-refuses-to-join-the-anti-china-coalition/; https://www.rferl.org/a/which-european-countries-support-the-5g-clean-network-initiative-/30928122.html

[6] The archived US DoS website cited in note 5 above shows that Clean Network include: 11 of 12 Three Seas nations. Among non-EU and NATO Allies, Albania, Canada, North Macedonia and Norway and UK can be confirmed as countries joining the program on relevant websites. As for other regions, Australia, Brazil, Georgia, India, Israel, Japan, Kosovo, New Zealand, Nauru, Dominica Republic, Ecuador, Eswatini, Ukraine can also be confirmed as member countries (region) of the program.

[7] The two NATO nations may be Iceland, Montenegro or Turkey.

[8] '5G-front: Hungary Refuses to Join the Anti-China Coalition,' *Dairy News Hungary*, 18 November 2020, https://dailynewshungary.com/hungarian-foreign-ministry-refuses-to-join-the-anti-china-coalition/

Whether the network hardware and software suppliers are subject, without independent judicial review, to control by a foreign government. [emphasis added][9]

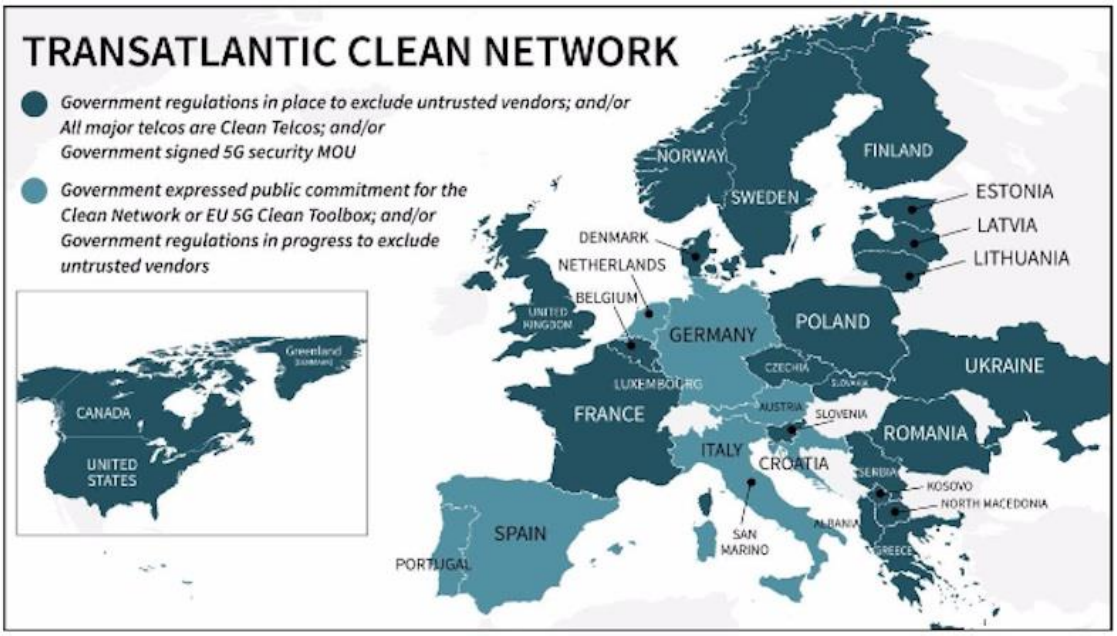

Figure 1: Member countries of Clean Network[10]

The Clean Network Alliance is merely a political pledge but it may have a significant effect on each country's decision on which companies are considered 'untrusted', given that the US government at that time was explicit about the vision. It is no surprise that some European countries including Estonia,[11] Poland,[12] Romania[13] and Sweden[14] have imposed a ban on Chinese companies entering the 5G network market or are in the process of implementing it.

[9] 'United States – Slovak Republic Joint Declaration on 5G Security,' 23 October 2020, https://2017-2021.state.gov/united-states-slovak-republic-joint-declaration-on-5g-security/index.html

[10] The US Embassy and Consulate in Greece, `The Transatlantic Alliance Goes Clean,´ https://gr.usembassy.gov/the-transatlantic-alliance-goes-clean/

[11] 'Legislation Barring Huawei 5G tech Passes Riigikogu,' *ERR News*, 25 November 2021, https://news.err.ee/1608414737/legislation-barring-huawei-5g-tech-passes-riigikogu

[12] 'Huawei Challenges Legality of 5G Bans in Poland, Romania,' *Politico*, 2 November 2020, https://www.politico.eu/article/huawei-hints-at-legal-action-against-5g-bans-in-poland-romania/

[13] 'Romanian President Signs Bill into Law to Ban Huawei from 5G,' *Reuters*, 11 June 2021, https://www.reuters.com/business/media-telecom/romanian-president-signs-bill-into-law-ban-huawei-5g-2021-06-11/

[14] 'Huawei Appeals Sweden's 5G Equipment Ban,' *5G Observatory*, 2 October 2021, https://5gobservatory.eu/huawei-appeals-swedens-5g-equipment-ban/; Finbarr Bermingham, 'Huawei 5G Ban is Upheld by Swedish Court in Further Blow to Chinese Telecoms Giant's European plans,' *South China Morning Post*, 23 June 2021, https://www.scmp.com/news/china/article/3138369/huawei-5g-ban-upheld-swedish-court-further-blow-chinese-telecoms-giants

3. EU

The need to build a framework dealing with the security of the supply chain of new technologies became evident in 2019 when a resolution of the European Parliament[15] referred to the security threats concerning the rising Chinese technological presence in the EU; the Huawei – ZTE issue. The threat prompted the Commission to call on member states to complete a coordinated national risk assessment of 5G network infrastructure and forward the results to both the EU Commission and ENISA.[16] The goal of the surveys was to highlight the main threats and threat actors affecting 5G networks as well as relevant technical and non-technical factors that could endanger their configuration and procurement process.[17]

The first practical attempt to identify remedies to these security challenges is the cybersecurity of 5G networks - EU Toolbox of risk mitigating measures ('the Toolbox') published by the NIS Cooperation group on 29 January 2020.[18] The Toolbox has been identified as the main EU 'risk mitigation policy instrument'[19] to recommend strategical, technical and supporting actions to address risks related to 5G networks and interdependencies between 5G networks and critical infrastructure across EU member states. Neither the Toolbox nor any other document names a supplier or country, but the vulnerabilities and risk scenario described in the EU Coordinated Risk Assessment Report identify both technical and non-technical threats originating from a foreign government.[20] The Toolbox itself is not a binding instrument, but rather a coordinated set of risk management best practices and member states have a strong reason to implement it.[21] However, it is up to individual member states to choose how to implement mitigation measures. They decide on what measures must be taken according to circumstances and their assessment of risks and in particular, which vendor or country poses threats and consequent gaps in existing national regulations. So far there has been a divergent approach across member states[22] and the high dependency on a single vendor persists.[23] A court case was pending at the International Centre for Settlement of Investment Disputes (ICSID) as *Huawei v Sweden*[24] at the time of writing. Sweden was

---

[15] 'Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them,' European Parliament, 12 March 2019, https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1577382&l=en&t=D

[16] European Commission, 'Shaping Europe's Digital Future,' European Commission, 26 March 2019, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks,

[17] European Commission, 'Security of 5G networks: EU Member States Complete National Risk Assessments,' European Commission, 19 July 2019, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_4266

[18] European Commission, 'Cybersecurity of 5G Networks - EU Toolbox of Risk Mitigating Measures,' 29 January 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[19] Piret Pernik, Taťána Jančárková, Kadri Kaska, Urmas Ruuto, Costel-Marius Gheorghevici and Henrik Beckvard, 'Research Report Supply Chain and Network Security for Military 5G Networks,' NATO CCDCOE, 2021, p. 9, https://ccdcoe.org/uploads/2021/10/Report_Supply_Chain_and_Network_Security_for_Military_5G_Networks.pdf

[20] European Commission, 'Member States Publish a Report on EU Coordinated Risk Assessment of 5G Networks Security,' 9 October 2019, https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049

[21] Janka Oertel, 'On 5G, Brussels is Up to the Job,' European Council on Foreign Relations, 3 February 2020, https://ecfr.eu/article/commentary_on_5g_brussels_is_up_to_the_job/

[22] 'EU Nations Divided on 5G Security, Auditors Say,' *Euractiv*, 8 January 2021, https://www.euractiv.com/section/5g/news/eu-nations-divided-on-5g-security-auditors-say/

[23] Pernik, Jančárková, Kaska, Ruuto, Gheorghevici and Beckvard, 'Research Report Supply Chain and Network Security for Military 5G Networks,' p. 9,

[24] ICSID, Huawei Technologies Co., Ltd. v. Kingdom of Sweden (ICSID Case No. ARB/22/2), https://icsid.worldbank.org/cases/case-database/case-detail?CaseNo=ARB/22/2

the first country in the EU to exclude Huawei products from the 5G network,[25] and Stockholm's Administrative Court of Appeal upheld a court of first instance's decision in June 2022.[26]

No single certification scheme yet exists to ensure the supply chain security of 5G networks, ICT products and cloud services but common candidate EU cybersecurity certification schemes are in development.[27] These are EU5G, [28] EUCC (Common Criteria-based European candidate cybersecurity certification scheme,[29] and EUCS (European Cybersecurity Certification Scheme for Cloud Services). Once these come into effect, they will supersede existing national schemes, although certification is voluntary.[30]

On 12 March 2019, the European Parliament asked the Commission to enlarge the scope of the NIS Directive to cover other critical sectors and services that are not covered by specific-sector legislation.[31] On 9 June 2020, the Commission welcomed the European Parliament's proposal and on 16 December 2020 circulated a new proposal for an empowered legal instrument that would repeal the NIS Directive 2016/1148.[32] This new proposal directly mentions cybersecurity and the protection of the supply chain of ICT services, systems and products. The new NIS Directive (NIS2) came into effect on 16 January 2023.

Its Chapter II Article 7 requires member states to include a specific policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services as part of their cybersecurity strategy. Article 21 expects essential and important entities of each Member State to take the risks management measures considering security-related aspects of the supply chain including the relationship between each entity, supplier or service provider such as data storage and processing services or managed security services. The aim is to strengthen control of the development procedures of the products and services used by member states' essential and important entities. Article 22 recognises the importance of the

---

[25] 'Huawei is Taking Sweden to Court After the Country Banned its 5G products,' *Euronews*, 31 January 2022, https://www.euronews.com/next/2022/01/31/huawei-is-taking-sweden-to-court-after-the-country-banned-its-5g-products

[26] 'Swedish Court Upholds Ban on Huawei Sale of 5G Gear,' *Reuters*, 22 June 2022, https://www.reuters.com/business/media-telecom/swedish-court-upholds-ban-huawei-sale-5g-gear-2022-06-22/

[27] ENISA, 'Securing EU's Vision on 5G: Cybersecurity Certification,' ENISA Press release, 3 February 2021, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

[28] ENISA, 'Ad-Hoc Working Group 03 - on 5G Cybersecurity Certification,' ENISA, 25 October 2021, https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification. The group focuses on specific use cases for cybersecurity certification such as the supply and deployment of identified 5G network equipment, management of subscriber identities, remote SIM provisioning, 5G authentication (including roaming) and subscriber connectivity services. ENISA, 'Call for Applications for the ad hoc Working Group on the Preparation of a Candidate EU 5G Cybersecurity Certification Scheme,' ENISA, June 2021.

[29] The Common Criteria (CC) is short for the Common Criteria for Information Technology Security Evaluation and it is the technical basis for the Common Criteria Recognition Arrangement (CCRA). It 'provid[es] a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products.' 'CC: 2022, Revision 1, Common Criteria for Information Technology Security Evaluation, CCMB-2022-11-001, ' November 2022, p. ix, https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf

[30] ENISA, 'EU Cybersecurity Certification – FAQ,' https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq/certification-schemes-and-cabs-faq

[31] European Parliament, 'Resolution of 12 March 2019 on Security Threats Connected With the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them (2019/2575(RSP)),' https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html

[32] European Commission, 'Proposal on Measures for a High Common Level of Cybersecurity Across the Union,' 16 December 2020, https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

Cooperation Group and ENISA in carrying out risk assessments of specific critical ICT services systems or products supply chains by considering both technical and non-technical factors. A newly created 'ICT Supply Chain Toolbox' is expected to complement the coordinated security risk assessments provided in Article 22(1), 'leveraging experiences from the 5G Toolbox and those gained at national level'.[33]

Further development was underway at the time of writing and the Commission has submitted a proposal for a regulation on cybersecurity requirements for products with digital elements known as the Cyber Resilience Act. It aims to improve supply chain security by imposing obligations and responsibilities on manufacturers, distributors and importers. These obligations include an assessment of the cybersecurity risks associated with a product with digital elements and drawing up of the technical documentation (including a cybersecurity risk assessment), an exercise of due diligence when integrating third-party-source components in products, effective handling of vulnerabilities and an undertaking a conformity assessments procedure under the Regulation (Article 10).[34]

[33] The Council of the European Union, 'Council Conclusions on ICT Supply Chain Security,' 17 October 2022, 13664/22, p. 13, para. 21, https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf

[34] European Commission, 'Cyber Resilience Act,' 15 September 2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

4. Four National Approaches to Controlling the Supply Chain Cybersecurity

Some nations have regulations with specific reference to 5G and others do not. The overview of regulatory measures in four countries analysed below includes both, based on publicly available information.

4.1 Finland

The relevant domestic law in Finland is the Act on Electronic Communications Services which was passed in 2020 and came into effect on 1 January 2021.[35] The aim of the reform is explained by the Finnish government as the implementation of EU instruments including the Toolbox.[36] Of particular note are the newly added provisions: Article 244a (Equipment used in critical parts of the communication network) and 244b (Network Security Advisory Board). Article 244a stipulates that a communications network device may not be used in a critical part of both the public telecommunications network and a dedicated network connected to the public communications network essential to vital functions of society, such as nuclear power plants, ports, airports if there are serious grounds to suspect that its use would endanger national security or defence in such a way as to enable foreign intelligence or activities to disrupt, paralyse or otherwise adversely affect Finland's vital interests or social order. According to a government proposal on an amendment submitted to Parliament on 11 June 2020, 'endanger[ing] national security' includes activities that threaten people's lives or health or the vital functions of society, the activities of a foreign state that may cause damages to Finland's international relations, economic or other important interest, or foreign intelligence activities.[37]

The Act aims only for 'the most critical parts of the network – understood as the most central nodes of network traffic'.[38] The Finnish Transport and Communications Agency (Traficom) issued a guidance[39] on 19 May 2021 (effective the next day) entitled `Regulation on Critical Parts of a Communications Network,´ which lists the functionalities of a communications network (Section 4), a 4G network (Section 5) and a 5G network (Section 5) as such. Telecommunications operators and dedicated network operators are required to identify critical parts

[35] The Act on Electronic Communication Services (Laki sähköisen viestinnän palveluista), 7.11.2014/917, Finlex (an online database of up-to-date legislative and other judicial information of Finland), https://www.finlex.fi/fi/laki/ajantasa/2014/20140917 (in Finnish)

[36] Ministry of Transport and Communications of Finland, press release, 'Act on Electronic Communications Services Enters Into Force on 1 January 2021,' Finnish Government website, 30 December 2020, https://valtioneuvosto.fi/en/-/act-on-electronic-communications-services-enters-into-force-on-1-january-2021

[37] 'The Government Proposal on the Amendment of the Act (Hallituksen esitys eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi),´ Finlex, p. 261, https://www.finlex.fi/fi/esitykset/he/2020/20200098 (in Finnish)

[38] Mikko Alkio and Petri Rouvinen, 'Implementing the 5G Toolbox: Could Finland Serve as a Model for the Other EU Countries?,' *Avance Insight*, January 2021, p. 5, https://www.avance.com/wp-content/uploads/2021/05/AVANCE-Insight-01-2021.pdf

[39] Traficom, Regulation on Critical Parts of a Communications Network (Viestintä: Määräys viestintäverkon kriittisistä osista), TRAFICOM/161584/03.04.05.00/2020, 19 May 2021, https://www.finlex.fi/data/normit/47015/Regulation_on_critical_parts_of_a_communications_network.pdf (Unofficial translation); https://www.finlex.fi/fi/viranomaiset/normi/480001/47015 (in Finnish).

and components and maintain up-to-date documentation. They are also required to assess whether a base station in their dedicated network constitutes a critical part, taking into consideration several factors[14], including geographical coverage and the base station's share of the network traffic (Section 3).

Traficom's roles under Article 244a of the Act also include providing advice to and consulting with the owners or operators of networks and ordering the removal of suspicious devices from their networks. The owners or operators have the right to compensation for removing devices.[40]

Under Article 244b, the Advisory Board for Network Security was set up in February 2021 to monitor the development of communications networks and technology and make proposals for improving network security.[41] The Board is chaired by the Director General of the Ministry of Transport and Communications and composed of representatives of the ministries of Foreign Affairs, Defence, Interior, Economic Affairs and Employment and Finance, and also of the private sector (see Figure 2).

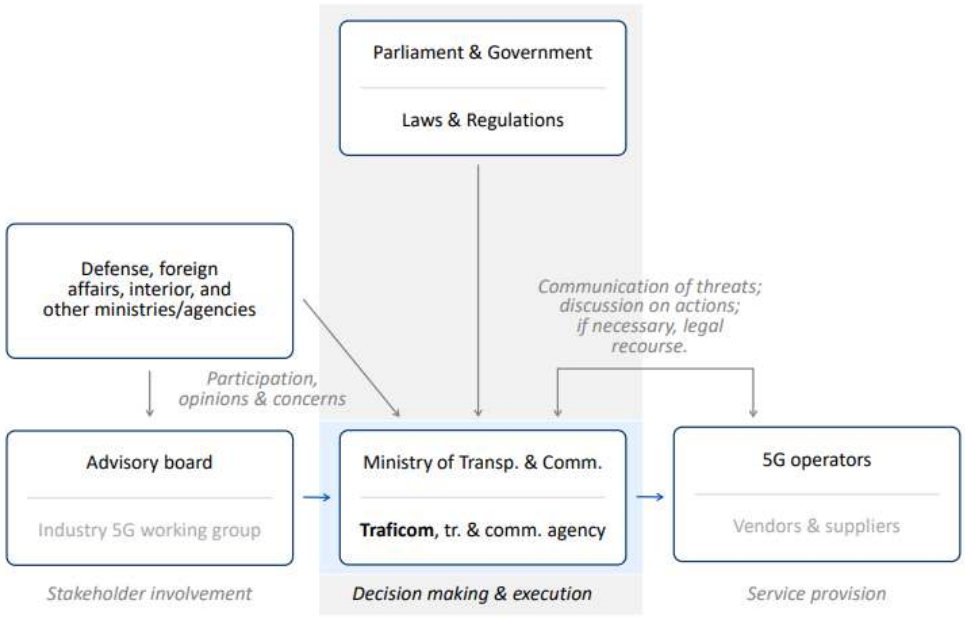

Figure 2: National framework in Finland regarding cybersecurity of 5G networks[42]

The Act does not name any particular company or country of origin as a banned actor[43] and it remains to be seen how the Act will be applied by the Finnish government. As yet there has been no confirmed case of removing a particular vendor in Finland but few if any Finnish companies or government organisations have purchased equipment from Chinese suppliers,[44] perhaps because a national supplier (Nokia) dominates the domestic market. However, assuming that Finland participated in the Clean Network programme and the joint declaration with the US is still valid, any device and equipment produced by Huawei or other Chinese vendors is unlikely to

[40] Ibid., p. 6.

[41] Ministry of Transport and Communications of Finland, press release, 'Advisory Board Set Up to Support Network Security,' https://valtioneuvosto.fi/en/-/advisory-board-set-up-to-support-network-security

[42] Alkio and Rouvinen, 'Implementing the 5G Toolbox: Could Finland Serve as a Model for the Other EU Countries?,' p. 6.

[43] 'Finnish Parliament Passes Law to Allow Banning Telecoms Equipment on Security Grounds,' *Telecompaper*, 9 December 2020, https://www.telecompaper.com/news/finnish-parliament-passes-law-to-allow-banning-telecoms-equipment-on-security-grounds-2--1364991

[44] An email correspondence by a Finnish government official to an inquiry from the author in the winter of 2021.

be procured for future networks and will be removed from existing networks, regardless of the Act being seemingly neutral to any particular country.

4.2 Japan

(A) Regulation Across the Government

There is no Japanese legislation in respect of government procurement of information systems and equipment and services, but there is a document entitled 'Understanding (Agreement) on Government Procurement Policy and Procurement Procedures for IT Goods and Services applies across government organisations'.[45] The Understanding was agreed upon on the 10th of December 2018[46] at a joint meeting of the Cybersecurity Measures Promotions Committee of (the Cybersecurity Strategic Headquarters (CSSH)) [47] and the Liaison Meeting of the Chief Information Officers (CIOs) of government agencies. In addition, all government ministries and agencies (25 in total), incorporated administrative agencies (IAAs)(87 in total)[48] and certain designated agencies under the Basic Act on Cybersecurity (9 in total) are also covered by the Understanding. The information systems, equipment and services covered under the Understanding are categorised into nine groups in Annex II: 1) communication line device, 2) server device, 3) terminal, 4) multifunction device (e.g., printer), 5) application-specific equipment, 6) software, 7) peripheral equipment, 8) external data storage medium, 9) services.

Under Annex III of the Understanding, these organisations are required to assess cybersecurity risks to the supply chain ahead of procurement procedures if the system is involved with national security and public order; the handling of classified information or sensitive information where leaking or manipulation may cause social or economic disruption; personal data; a LAN or foundation system that significantly affects government function in an event of suspension; or one with a high running cost.

They are also required to consult the National centre of Incident readiness and Strategy for Cybersecurity (NISC) and the Digital Agency for advice on mitigation measures and possible replacement with alternative items. According to the NISC, it advised 1,869 times in 2019 (risks were identified in 89 cases) and this rose to 3,325 in 2020 (risks in 190 cases).[49] However, further information on which vendors were thought to be causing concern

---

[45] 'Understanding (Agreement) on Government Procurement Policy and Procurement Procedures for IT Goods and Services (「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」),' 10 December 2018, last amended 2021, https://www.nisc.go.jp/active/general/pdf/choutatsu_moushiawase0901.pdf (only in Japanese).

[46] Japanese Ministry of Internal Affairs and Communications (MIC), ed., *White Paper: Information and Communication in Japan* (『情報通信白書令和２年版』), 2020, p. 37, https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2020/chapter-3.pdf (in English); p. 269, https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/n3400000.pdf (in Japanese)

[47] The CSSH was established under the Cabinet in 2015 and is in charge of setting out the standards of cyber security measures for government organisations, in addition to preparing a draft cybersecurity strategy (Article 26 (1) of the Basic Act on Cybersecurity (「サイバーセキュリティ基本法」), Act No. 104 of 2014). Japanese Law Translation Database System, https://www.japaneselawtranslation.go.jp/en/laws/view/3677 ; See organisation chart about the CSSH, https://www.nisc.go.jp/eng/pdf/Implementation_Framework.pdf

[48] The Act on General Rules for Incorporated Administrative Agencies (「独立行政法人通則法」, Act No. 103 of 1999), as amended as Act No. 66 of 2014, Japanese Law Translation Database System, https://www.japaneselawtranslation.go.jp/ja/laws/view/2754#je_ch1sc1at2

[49] 30th meeting of the CSSH, 7 July 2021, Material 8 `Amendment of the Understanding,´ p. 2, NISC, https://www.nisc.go.jp/conference/cs/dai30/pdf/30shiryou08.pdf (only in Japanese).

is not publicly available. The Chinese embassy in Tokyo reportedly showed discontent with the new guidance[50] although the Understanding does not name a vendor or country.[51]

Concerning 5G, spectrum allocation started in April 2019 with four mobile carriers. The Ministry of Internal Affairs and Communications (MIC), as the regulator, imposed conditions on the required level of cybersecurity measures for the supply chain, referencing the Understanding when approving rollout plans submitted by the carriers.[52] The Understanding also has become a requirement to be met for 5G network system operators when they apply for a loan and tax breaks under Article 7 of the Act on Promotion of Developing, Supplying and Introducing Systems Making Use of Specified Advanced Information and Communications Technologies of 2020.[53]

(B) Regulations at the MOD

The MOD is subject to the Understanding along with other government organs but has another standard : an effect on mission execution by the Japanese Self-Defense Forces (JSDF) which requires special provisions for supply chain security in a specification sheet for a tender, depending on the level of the impact.[54] For critical defence equipment, suppliers are required to submit the company's information on management, how to ensure supply chain security and audit. Suppliers are also strongly encouraged to offer products that meet Common Criteria Evaluation Assurance Levels (EAL) level 4.[55] The MOD also seeks the NISC's advice on procurements including on items listed in the Understanding, except for domestic products and that in use by US forces in

---

[50] 'Japan Bans Huawei and its Chinese Peers from Government Contracts: Move Aligns with US, Prompting 'Serious Concerns' and Protests of 'Discrimination',' *Nikkei Asia*, 10 December 2018, https://asia.nikkei.com/Economy/Trade-war/Japan-bans-Huawei-and-its-Chinese-peers-from-government-contracts

[51] Press Conference by Minister Seko (excerpted version. Provisional translation), Japanese Ministry of Economy, Trade and Industry (METI), 14 December 2018, https://www.meti.go.jp/english/speeches/press_conferences/2018/1214001.html; 'Japan Sets Policy That Will Block Huawei and ZTE from Public Procurement as of April,' *Japan Times*, 10 December 2018, https://www.japantimes.co.jp/news/2018/12/10/business/japan-sets-policy-will-block-huawei-zte-public-procurement-april/

[52] MIC, 'Approval of Plans on Setting Up of 5G Specific Base Stations,' April 2019, p. 15, https://www.soumu.go.jp/main_content/000613734.pdf (only in Japanese).

[53] 'Cabinet Decision on the Bill for the Act on Promotion of Developing/Supplying and Introducing Systems Making Use of Specified Advanced Information Communication Technologies (「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律」),' METI, 18 February 2020, https://www.meti.go.jp/english/press/2020/0218_001.html; See the Act, https://elaws.e-gov.go.jp/document?lawid=502AC0000000037 (only in Japanese).

[54] 'Notice by the Vice-Minister of Defense, on Measures for Addressing Supply Chain Risks Involving Procurement of Information Systems (防衛事務次官「情報システムに関する調達に係るサプライチェーン・リスク対応のための措置について（通達）」),' 31 January 2019, last amended on 29 March 2019, https://www.mod.go.jp/gsdf/tercom/img/file503.pdf; 'General Notice by the Commissioner of the Acquisition, Technology & Logistics Agency (ATLA) of Japan MOD, on Measures for Addressing Supply Chain Risks Involving Procurement of Information Technology (IT)-assisted Defense Equipments and Associated Services (防衛装備庁長官「IT 利用装備品等及び IT 利用装備品等関連役務の調達におけるサプライチェーン・リスクへの対応について（通知）」),' 21 January 2021, last amended on 31 March 2021, https://www.mod.go.jp/j/procurement/seido/buppin_ekimu/pdf/zenpan_04.pdf (both only in Japanese). These internal MOD documents do not list a specific country or company.

[55] 'General Notice by the Commissioner of the ATLA of Japan MOD, on Details of Measures for Addressing Supply Chain Risks Involving Procurement of Information Systems (防衛装備庁長官「情報システムに関する調達に係るサプライチェーン・リスク対応のための措置の細部事項について（通知）」),' 9 January 2019, last amended on 31 March 2021, http://www.clearing.mod.go.jp/kunrei_web/ (only in Japanese).

Japan.[56] A senior MOD official explained at the National Diet in June 2022 that no Chinese products have been acquired by the MOD, at least since the Understanding came into effect.[57]

4.3 United Kingdom[58]

(A) MOD's Cyber Security Model

A consideration of the cybersecurity risk in the supply chain is found in the *National Cyber Security Strategy* published in 2011.[59] In respect of the MOD's policy on defence procurement, an application of the mandatory Cyber Essentials Scheme was extended to all MOD suppliers from 1 January 2016 onward.[60] Suppliers for the MOD are required to be certified to bid for contracts.[61]

The MOD has had a mandatory Cyber Security Model (CSM) in place since 2017 to protect MOD Identifiable Information[62] from the cyber threat.[63] The CSM comprises three steps: risk assessment, a supplier assurance questionnaire (SAQ) to be completed by suppliers to show suppliers meet the requirements of this risk,[64] and an assessment of the SAQ by the authority. In the case of the contract between the MOD and the supplier, the MOD is the authority. The supplier becomes the authority for a contract between them and a sub-contractor.[65]

---

[56] An interview to the Japan MOD officials in charge by the author on 13 October 2022.

[57] Answer by the Japan MOD senior official Mr. Hideki Tsuchimoto (土本政府参考人). The Minute of Committee of National Security, the House of Representative, 208th Session of the National Diet, 3 June 2022, https://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/001520820220603007.htm (only in Japanese).

[58] The NCSC has released guidance on how organisations can control and oversight their supply chain. NCSC, 'Supply Chain Security Guidance,' 28 January 2018, https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

[59] *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, November 2011, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf: The Strategy 2016-2021 repeat the same policy by describing 'all suppliers to the Government meet appropriate cyber security standards.' The National Cyber Security Strategy 2016 to 2021, 2016, p. 38, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[60] UK NCSC, 'About Cyber Essentials,' https://www.ncsc.gov.uk/cyberessentials/overview

[61] UK Cabinet Office, Procurement Policy Note – Cyber Essentials Scheme. ACTION NOTE 09/14, 25 May 2016, p. 1, https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification

[62] MOD Identifiable Information' means all Electronic Information which is attributed to or could identify an existing or proposed MOD capability, defence activities or personnel and which the MOD requires to be protected against loss, misuse, corruption, alteration and unauthorised disclosure. UK MOD, 'Guidance: Cyber DEFCON 658,' 10 September 2021, https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down/cyber-defcon-658#definitions-1

[63] UK MOD, 'Guidance: DCPP: Your Questions Answered,' 26 October 2017, 'https://www.gov.uk/government/publications/defence-cyber-protection-partnership-your-questions-answered/dcpp-your-questions-answered-html

[64] UK MOD, 'Guidance Cyber Security Model: Cyber Risk Profiles' Requirements,' 24 March 2015, updated 24 July 2020, https://www.gov.uk/government/publications/defence-cyber-protection-partnership-cyber-risk-profiles

[65] The UK Government, 'DCPP Cyber Security Model: Industry Buyer and Supplier Guide,' 30 March 2017, last updated 22 June 2018, p. 3, https://www.gov.uk/government/publications/dcpp-cyber-security-model-industry-buyer-and-supplier-guide

(B) Telecommunications (Security) Act 2021

Huawei used to be the largest vendor until July 2019 when *UK Telecoms Supply Chain Review Report*[66] was published. The cybersecurity risk from Huawei was described as 'moderate' in the report, although its ties with the Chinese government under the Chinese National Intelligence Law 2017 were noted.[67] In January 2020, the UK government announced a new plan for 5G and full-fibre networks which would exclude Huawei as a high-risk vendor (HRV) from security-critical network functions and sensitive locations and limit it to a minority presence in other network functions up to a cap of 35%.[68] In July 2020, the UK government updated its plan following the National Cyber Security Centre's (NCSC) analysis of an additional sanction imposed by the US Department of Commerce on Huawei on 15 May that year[69] and decided that the procurement of Huawei equipment should be banned from 31 December and that all Huawei equipment should be removed from 5G networks by 2027.[70] The report included proposals to the government for the UK to have a new robust security framework for 5G, a full-fibre network, and new legislation for cyber security in the telecoms sector.[71] The Telecommunications (Security) Bill 2021 was introduced to Parliament by the government on 24 November 2020 and passed into law on 17 November 2021.[72]

The Act brings a new duty on providers to take security measures to identify and reduce the risks of security compromises and prepare for such compromises (Section 105A).[73] The Office of Communications is provided with a wide range of powers and responsibilities such as assessing and enforcing providers' compliance with their security duties (Sections 6 and 7), reporting to the Secretary of State on security-related matters (Section 11), requiring and sharing security-related information (Section 12), monitoring a provider's compliance with a designated vendor direction (including inspection) and reporting this information to the Secretary to State (Sections 18 and 19).

The Act gives new powers to the Secretary of State to handle the risks posed by HRVs if there is no way of mitigating the threat. Under Section 105Z8 (3), the Secretary of State may issue a designation notice if they consider it necessary in the interests of national security, taking account of various factors listed in subsection (4) (a)-(l),[74] including:

- the strategic position or scale of the vendor in UK networks;

- the strategic position or scale of the vendor in other telecoms networks, particularly if the vendor is new to the UK market;

---

[66] The UK Secretary of State for Digital, Culture, Media and Sport, 'UK Telecoms Supply Chain Review Report,' July 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

[67] Ibid., p. 25, paras. 3. 15-3. 16.

[68] 'Foreign Secretary's Statement on Huawei,' 28 January 2020, https://www.gov.uk/government/speeches/foreign-secretary-statement-on-huawei; Examples of network functions are listed in the NCSC guidance, para. 11. NCSC, 'NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks,' 28 January 2020, https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

[69] NCSC, 'Summary of the NCSC Analysis of May 2020 US Sanction,' NCSC, 14 July 2020, https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction

[70] Press release, 'Huawei to be Removed from UK 5G Networks by 2027,' UK government website, 14 July 2020, https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027

[71] The UK Secretary of State for Digital, Culture, Media and Sport, 'UK Telecoms Supply Chain Review Report,' p. 6.

[72] Telecommunications (Security) Act 2021, https://www.legislation.gov.uk/ukpga/2021/31/enacted

[73] Ibid., Section1, https://www.legislation.gov.uk/ukpga/2021/31/section/1/enacted; Explanatory Notes, p. 12.

[74] Telecommunications (Security) Act 2021, Section 16, https://www.legislation.gov.uk/ukpga/2021/31/section/16/enacted

- the quality and transparency of the vendor's engineering practices and cyber security controls;

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

- security laws in the jurisdiction where the vendor is based and the risk of external direction that conflicts with the interests of national security (emphasis added);

- the relationship between the vendor and the vendor's domestic state apparatus; and

- the availability of offensive cyber capability by that domestic state apparatus, or associated actors, that might affect the national security of any country or territory.[75]

Section 105Z1 provides that the Secretary of State may issue a 'designated vendor direction' to a public communication provider regarding requirements on their use of goods, services, or facilities supplied by a vendor designated under section 105Z8 only if considered necessary in the interests of national security by the Secretary of State and proportionate to what is sought to be achieved by the direction in subsections (1) and (2).[76] On receipt of a direction, a public communications provider must comply with it (Section 105Z1(7)). In case of non-compliance, the Secretary of State may issue a notification of contravention to a provider, in which the penalty is shown (Section 105Z18). The penalty amount is either 10 % of the turnover of a provider's relevant business for the relevant period (Section 105Z19, subsection (2)), or £100,000 per day when the contravention continues (ibid., subsection (3)).[77] A Huawei Draft Designation notice and Huawei Draft Designated Vendor Direction were published on the UK government website in November 2020 and its final version was issued October 2022.[78] The Designation Notice, in particular, cited cyberattacks by the Chinese State and associated actors, harmful activities enabled by Chinese laws including the National Intelligence Law 2017, the concerning quality of both cyber security and engineering on Huawei´s products and services and the US sanctions imposed against Huawei, as giving rise to unacceptable risks to national security.[79]

In May 2021, the UK government released the *Supply Chain Cyber Security Call for Views* to seek insight across the industry, in particular, on how to effectively manage supply chain cybersecurity risks arising out of contracting Managed Service Providers. Many respondents pointed out that cloud and software vendors can be a key source of supply chain risk to customer organisations by providing attractive targets to malicious actors. They also claimed that they were in a weak position to be able to request information or require more stringent cyber security practices and that the lack of cybersecurity standards such as certification or audit systems was enabling new providers with inadequate practices to enter the UK market. As a result, many respondents gave a positive perspective on increasing government intervention. Of particular note is 'setting minimum requirements (on Managed Service Providers) in public procurement' (92% of respondents responded as effective), 'developing

[75] Explanatory Notes, pp. 9-10, https://www.legislation.gov.uk/ukpga/2021/31/notes/contents

[76] Telecommunications (Security) Act 2021, Section 15, https://www.legislation.gov.uk/ukpga/2021/31/section/15/enacted

[77] Ibid., Section 20, https://www.legislation.gov.uk/ukpga/2021/31/section/20/enacted

[78] 'Policy Paper: Telecommunications (Security) Bill: Illustrative Designated Vendor Direction and Designation Notice,' UK government website, 30 November 2020, https://www.gov.uk/government/publications/telecommunications-security-bill-illustrative-designated-vendor-direction-and-designation-notice

[79] 'Designation Notice under Section 105Z8 of the Communications Act 2003 Designating Huawei for the Purposes of a Designated Vendor Direction,' 12 October 2022, pp. 1-3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1110247/Final_Huawei_Designation_Notice.pdf

new or updated legislation' (82%), and 'creating a set of target regulatory guidance to support critical infrastructure sector regulations' (92%).[80]

4.4 United States

The US is the most extensive in addressing supply chain cybersecurity problems. Its regulatory measures are expanding, ranging from export restrictions to a ban on procuring Chinese equipment in the US network system, an action that dates back more than a decade.[81] This section only touches on regulatory measures associated with the supply chain.

(A) Export Restrictions

US practice on export restrictions has affected other countries' policies including the UK's *Telecom Supply Chain Review Report*. The US Export Administration Regulation was amended on 16 May 2019 to add Huawei and 68 non-US affiliates of Huawei based on its conclusion that Huawei's activities are contrary to the US national security or foreign policy interest.[82] As a result of the additions, the export, re-export, or transfer (in-country) of any item subject to the Export Administration Regulations (EAR) to Huawei or any of its affiliates was restricted. The motivation behind the decision was that Huawei and its affiliates were indicted in federal court on thirteen counts for violations of the International Emergency Economic Powers Act (IEEPA) and conspiracy to violate the Act concerning transactions with Iran.[83] On 15 May 2020, the Department of Commerce announced further restrictions given that the use by Huawei of US software and technology continued after its addition to the Entity List. The foreign-produced direct product rule was amended to prevent Huawei from using US technologies in semiconductor production,[84] which influenced the UK government's decision to ban Huawei in the UK.[85]

(B) Transactions Prohibitions

In Executive Order (EO) 13873 of 15 May 2019,[86] President Trump declared a national emergency, finding that foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communication technology and services and committing malicious cyber-enabled actions, including economic and industrial

---

[80] 'Policy Paper: Government Response to the Call for Views on Supply Chain Cyber Security,' UK government website, 15 November 2021, https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security/government-response-to-the-call-for-views-on-supply-chain-cyber-security

[81] Stephen P. Mulligan and Chris D. Linebaugh, 'Huawei and U.S. Law,' Congressional Research Service, R46693, 23 February 2021, pp. 3-5, https://sgp.fas.org/crs/misc/R46693.pdf

[82] Bureau of Industry and Security (BIS) of the US Department of Commerce, Addition of Entities to the Entity List, *Federal Register*, Vol. 84, 21 May 2019, p. 22961, https://www.govinfo.gov/content/pkg/FR-2019-05-21/pdf/2019-10616.pdf

[83] The US Department of Justice, press release, 'Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud,' 28 January 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial

[84] The US Department of Justice, press release, 'Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies,' 15 May 2020, https://2017-2021.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts.html

[85] Explanatory Notes, p. 7, para. 19, https://www.legislation.gov.uk/ukpga/2021/31/notes/contents

[86] Executive Order 13873 of 15 May 2019 on Securing the Information and Communications Technology and Services Supply Chain, *Federal Register*, Vol. 84, 17 May 2019, p. 22689, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

espionage against the US. To address this threat, the acquisition, importation, transfer, and installation were prohibited when the Secretary of Commerce, in consultation with other agency heads, determined that:

(i) The transaction involves [ICTS] designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) The transaction:

(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of ICTS in the US;

(B) poses an undue risk of catastrophic effects on the security or resilience of US critical infrastructure or the digital economy of the US; or

(C) otherwise poses an unacceptable risk to the national security of the US or the security and safety of US persons.[87]

Reportedly, the US government intended to apply the Order to Huawei, by adding it and its affiliates to the Entity List at the same time that the Order was issued, although White House officials denied that claim.[88]

On the 9th of June 2021, Executive Order 14034 was issued to elaborate on additional measures to be taken under EO 13873, in particular, to address the risks related to connected software applications (CSA).[89] Unlike the previous Order, EO 14034 names China as a foreign adversary as it 'among others, continues to threaten the national security, foreign policy and economy of the US.' The Order also listed potential indicators to consider when evaluating CSA-related risks. The following are especially foreign adversary-related risks:

- ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities;

- use of the [CSA] to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data;

- ownership, control, or management of [CSA] by persons subject to coercion or cooption by a foreign adversary.[90]

(C) Prohibitions on the Use of Risky Equipment and Services in Federal Procurement[91]

The National Defense Authorization Act for Fiscal Year 2018 (2018 NDAA) banned the Defense Department from procuring or obtaining equipment or services from Huawei or ZTE for anything involved with nuclear deterrence

[87] Ibid., pp. 22689-22690.

[88] 'US Bans Huawei from Selling Telecom Gear and Threatens its Supply Chain,' *CNN*, 16 May 2019, https://edition.cnn.com/2019/05/15/tech/trump-executive-order-telecom-security/index.html; Mulligan and Linebaugh, 'Huawei and U.S. Law,' p. 15.

[89] The US Department of Commerce, 'ICT Supply Chain: Securing the Information and Communications Technology and Services Supply Chain,' https://www.commerce.gov/issues/ict-supply-chain#:~:text=14034)%2C%20on%20November%2023%2C,2021%20(86%20FR%204909 ; Executive Order 14034 of 9 June 2021 on Protecting Americans' Sensitive Data From Foreign Adversaries, *Federal Register*, Vol. 86, 11 June 2021, p. 31423, https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries ; as for the background information, the US Department of Commerce, 'ICT Supply Chain,' https://www.commerce.gov/issues/ict-supply-chain

[90] EO 14034, p. 31423. Other indicators are as follows: ownership, control, or management of [CSA] by persons involved in malicious cyber activities; a lack of thorough and reliable third-party auditing of [CSA]; the scope and sensitivity of the data collected; the number and sensitivity of the users of the [CSA]; and the extent to which identified risks have been or can be addressed by independently verifiable measures.

[91] See also Mulligan and Linebaugh, 'Huawei and U.S. Law,' pp. 19-25.

or homeland defence.[92] It also prohibited all federal entities from using any hardware, software or services provided by Kaspersky Lab, any successor entity or entity associated with Kaspersky.[93] Kaspersky has already its encryption technologies certified as compliant with the Federal Information Processing Standards (FIPS) 140-2 in 2016.[94] Shortly after the NDAA was signed by the President, two Kaspersky entities filed complaints at the District Court for the District of Columbia, which granted the government's motions to dismiss. The Court of Appeals upheld the District Court's dismissal.[95] The 2019 NDAA expanded its list of equipment vendors by adding three other Chinese companies. All executive agencies were prohibited from purchasing and obtaining equipment and using a loan or granting funds for that purpose from Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company and Dahua Technology Company (their subsidiary and affiliates included) in addition to Huawei and ZTE.[96] Huawei filed a complaint similar to that of Kaspersky in the District Court for the Eastern District of Texas in 2019 to invalidate the NDAA, but its claim was denied.[97]

The Federal Communications Commission's (FCC) initiative began in April 2018 when it proposed 'targeted action' at particular vendors to safeguard US communications networks against a national security threat. Assessing the discussions over the past couple of years at the White House, Congress and the 2018 NDAA, the FCC proposed a rule that certain federal funds (in this case, Universal Service Funds (USF)) may not be used to purchase or obtain any equipment or services that pose a threat to the integrity of communications networks or the communications supply chain and sought comments on how to implement and enforce it.[98] It cited as legal authority the United States Code, Title 47, Sections 201 (b)[99] and 254. After collecting inputs and looking at further restrictions imposed by the government on Huawei and ZTE, the FCC made an initial designation of these

---

[92] Public Law No. 115-91, Section 1656 [Security of nuclear command, control and communications system from commercial dependencies], the Law Library of US Congress, https://www.congress.gov/bill/115th-congress/house-bill/2810/text

[93] Section 1634 of the 2018 NDAA.

[94] Kaspersky Lab, 'Kaspersky Lab's Corporate Data Protection Technology is FIPS 140-2 Certified,' 30 November 2016, https://www.kaspersky.com/about/press-releases/2016_kaspersky-lab-s-corporate-data-protection-technology-is-fips-140-2-certified

[95] Kaspersky Lab, Inc. et al v. Department of Homeland Security et al, US Court of Appeals for the District of Columbia Circuit, Nos. 1:17-cv-17-2697 and 1:18-cv-325, 909 F.3d 446, 453-64 (D.C. Cir. 2018), https://cases.justia.com/federal/appellate-courts/cadc/18-5176/18-5176-2018-11-30.pdf?ts=1543591852

[96] Public Law No. 115-232, Section 889 [Prohibition on certain telecommunications and video surveillance services or equipment], the Law Library of US Congress, https://www.congress.gov/bill/115th-congress/house-bill/5515/text;
As for more detail regarding 2018 NDAA and 2019 NDAA, Jill C. Gallagher,' U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy and Economic Interests,' Congressional Research Service, R47012, 5 January 2022, pp. 12-22, https://www.everycrsreport.com/files/2022-01-05_R47012_65c5c54827b8fef912a19079f10e144b3b88d009.pdf

[97] Memorandum Opinion and Order, Huawei Technologies USA, Inc., et al. v. The United States of America, et al., 13 , U.S. District Court for the Eastern District of Texas, No. 4:2019-cv-00159 - Document 51 (E.D. Tex. 2020), https://law.justia.com/cases/federal/district-courts/texas/txedce/4:2019cv00159/188186/51/

[98] FCC, 'Notice of Proposed Rulemaking: Protecting Against National Security Treats to the Communications Supply Chain Through FCC Programs,' 18 April 2018, p. 6, para. 13, https://www.fcc.gov/document/fcc-proposes-protect-national-security-through-fcc-programs-0

[99] 'The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter [on Wire or Radio Communication].' The U.S. Government Publishing Office, p. 43, https://www.govinfo.gov/content/pkg/USCODE-2021-title47/pdf/USCODE-2021-title47-chap5-subchapII-partI-sec201.pdf#:~:text=(b)%20All%20charges%2C%20practices,communications%20by%20wire%20or%20radio

two vendors and their affiliates as national security risks on 22 November 2019 [100] and final designations on the same vendors on 30 June 2020.[101] Huawei's attempt to overturn FCC's designation was unsuccessful.[102]

The list of covered vendors for this purpose (the Covered List) was updated on 12 March 2021 under the Secure and Trusted Communications Networks Act of 2019,[103] and Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company and Dahua Technology Company were added under the 2019 NDAA.[104]

For equipment and services to be listed in the Covered List, they must meet the following requirements pursuant to section 2(b) (2) of the Secure and Trusted Communications Networks Act:

> section 2(b)(2) [communication equipment of services] capable of-
>
> (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles:
>
> (B) causing the network of a provider of advanced communications service to be disrupted remotely; or
>
> (C) otherwise posing an unacceptable risk to the national security of the US or the security and safety of US persons.

Under the Code of Federal Regulations Title 47, § 1.50002,[105] a determination to update the Covered List is to be made by any executive branch interagency body or the Department of Commerce under Executive Order no. 13873; or in line with Section 889 of the 2019 NDAA; or a specific determination made by an appropriate national security agency.

The Secure and Trusted Communications Networks Act also set up a reimbursement programme (Secure and Trusted Communications Networks Reimbursement Programme (SCRP)) to reimburse eligible providers for the cost of removal, replacement, and disposal of equipment and services provided by Huawei or ZTE that was obtained on or before 30 June 2020.[106]

---

[100] FCC, First Report and Order, Order and Further Notice of Proposed Rulemaking, adopted on 22 November 2019, WC Docket No. 18-89, PS Docket Nos. 19-351, 19-352, 34 FCC Rcd 11423 (14), https://www.fcc.gov/document/protecting-national-security-through-fcc-programs-0

[101] FCC, Public Notice, 'Public Safety and Homeland Security Bureau Issues Final Designations of Huawei Technologies Company and ZTE Corporation as Companies Posing a National Security Threat to the Integrity of Communications Networks and the Communications Supply Chain,' PS Docket Nos. 19-351, 19-352, https://www.fcc.gov/document/fcc-designates-huawei-national-security-threat

[102] Huawei Technologies v. FCC & USA on Petition for Review of an Order of the FCC, No. 19-60896, US Court of Appeals for the Fifth Circuit, 18 June 2021, https://docs.fcc.gov/public/attachments/DOC-373457A1.pdf

[103] Public Law No. 116-124, the Law Library of US Congress, https://www.congress.gov/bill/116th-congress/house-bill/4998/text

[104] FCC, List of Equipment and Services Covered By Section 2 of The Secure Networks Act, https://www.fcc.gov/supplychain/coveredlist

[105] 47 CFR § 1.50002, https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-1/subpart-DD/section-1.50002

[106] On 27 December 2020, the Consolidated Appropriations Act of 2021 was enacted in order to appropriate $1.9 billion to 'carry out' the SCRP and to amend the Program's eligibility to add smaller providers with 10 million or fewer subscribers (FCC, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, *Federal Register*, Vol. 86, 6 October 2021, pp. 55515-55516, https://www.govinfo.gov/content/pkg/FR-2021-10-06/pdf/2021-21783.pdf). The application for reimbursement was due on 28 January 2022 on the dedicated website of FCC (FCC, 'Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,' https://www.fcc.gov/supplychain).

On 11 November 2021, the Secure Equipment Act of 2021 was enacted[107] requiring that equipment and services purchased with private funds be subject to FCC authorisation[108] and thereby FCC shall no longer review any application for equipment authorisation for Huawei and other Chinese vendors' equipment on the Covered List (section 2. (a)(2)). More additions of Chinese products are planned. However, an expert criticises the Act arguing that the Act is 'woefully deficient in size and scope' by leaving out components in Apple or HP laptops or off-brand inexpensive IoT devices.[109]

(D) Prohibition on Use of Risky Software in Federal Procurement

On 12 May 2021, Executive Order 14028 on Improving the Nation's cybersecurity was signed by President Biden.[110] Section f of the Order focuses on the supply chain security of software procured by federal agencies, with a particular emphasis on 'critical software'; software that performs functions critical to trust (Sec.4 (a)). The Order assigned the National Institute of Standards and Technology (NIST) several tasks and all the assignments were complete at the time of writing.[111]

The Federal Acquisition Regulation (FAR) is subject to review by the Secretary of Homeland Security to the FAR Council regarding contract language[112] in federal procurement (Sec. 4 (o)). The amendment aims to 'provide contracting officers with a single, consolidated location in the FAR for cybersecurity supply chain risk management requirements' and the process was still underway at the time of writing with a progress report due 29 March 2023.[113] After amendment of the FAR, federal agencies will be required to remove software that does not meet the requirements of the amended FAR (Sec. 4 (p)).

The Order also made it mandatory to create a Software Bill of Materials (SBOM) for a software package, which will help mitigate risks of software supply chain security.[114]

---

[107] Public Law No. 117-55, the Law Library of US Congress, https://www.congress.gov/117/plaws/publ55/PLAW-117publ55.pdf

[108] Report of the House Committee on Energy and Commerce, 19 October 2021, p. 2, the Law Library of US Congress, https://www.congress.gov/congressional-report/117th-congress/house-report/148/1

[109] Roslyn Layton, 'Secure Equipment Act Becomes Law,' *Forbes*, 1 December 2021, citing a comment by Joseph Steinberg. https://www.forbes.com/sites/roslynlayton/2021/12/01/secure-equipment-act-becomes-law/

[110] *Federal Register*, Vol. 86, 17 May 2021, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[111] NIST, 'Fact Sheet: Executive Order on Improving the Nation's Cybersecurity,' May 2022, https://www.nist.gov/system/files/documents/2022/05/24/EO%20Fact%20Sheet.pdf

[112] A contract language means a language used in 'Federal Government-wide Acquisition Contracts.' The US White House, 'Executive Order on Improving the Nation's Cybersecurity,' 12 May 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[113] The US DoD, 'Open FAR Cases as of 3/24/2023,' 24 March 2023, p. 4, https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

[114] After the National Telecommunications and Information Administration (NTIA) published 'The Minimum Elements For a [SBOM] in accordance with the Order sec. 4 (f), the Enduring Security Framework (ESF) has published Recommended Practices Guide for both developers and suppliers in the autumn 2022, https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Cybersecurity-Partnerships/ESF/

5. United Nations

The UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security is the first multinational forum to deal with the topic of the cybersecurity of the supply chain.[115] The supply chain is referred to in both the 2011[116] and 2015[117] versions of the International Code of Conduct for Information Security proposed by China, Russia, Tajikistan, Uzbekistan and other nations participating in the Shanghai Cooperation Organisation (SCO). Yet these proposals did not lead to further discussion at the UN.

Following the 2013[118] and 2015 reports,[119] the UN GGE 2021 Report elaborates on the supply chain more in the context of a norm for the responsible behaviour of states. Its Norm 13(i) repeats paragraph 13(i) of the 2015 report by providing that 'States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions'[120] and subsequent paragraphs 56-59 list 'an additional layer of understanding (of GGE) to' the norm as follows [emphasis added]:

> Para. 57 Reasonable steps can include:
>
> (a) Putting in place at the national level comprehensive, transparent, objective and impartial frameworks and mechanisms for supply chain risk management;
>
> (b) Establishing policies and programmes to objectively promote the adoption of good practices by suppliers and vendors of ICT equipment and systems;
>
> (c) Increased attention in national policy and in dialogue with States and relevant actors at the UN and other fora on how to ensure all States can compete and innovate on an equal footing;
>
> (d) Cooperative measures such as exchanges of good practices […] on supply chain risk management; developing and implementing globally interoperable common rules and standards for supply chain security.
>
> In relation to the second paragraph of Norm 13 (i), para. 58 recommends:
>
> (a) States may also consider establishing independent and impartial certification processes.
>
> (b) Legislative and other safeguards that enhance the protection of data and privacy.
>
> (c) Measures that prohibit the introduction of harmful hidden functions and the exploitation of vulnerabilities in ICT products.

Thus, each country is urged to take reasonable steps such as setting up national frameworks and mechanisms including the certification process, and developing international rules and standards to ensure the integrity of the supply chain. The concept of Norm 13(i) of the GGE 2021 Report is shared in paragraph 28 of the Final

---

[115] Oleg Demidov and Giacomo Persi Paoli, 'Supply Chain Security in the Cyber Age, UNIDIR, 2020, pp. 47-48, https://unidir.org/sites/default/files/2020-02/Supply%20Chain%20Security%20in%20the%20Cyber%20Age%20-%20UNIDIR%20Report.pdf

[116] A/66/359, https://undocs.org/A/66/359

[117] A/69/723, https://undocs.org/en/A/69/723

[118] A/68/98, https://undocs.org/A/68/98

[119] A/70/174, https://undocs.org/A/70/174

[120] A/76/135, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement

Substantive Report the Open-Ended Working Group (OEWG) adopted unanimously in March 2021,[121] which means that there is consensus among UN member states but not on what common rules and standards would be developed. National approaches like those of the UK and the US will encounter objections from China and other nations sympathetic to China, which may hinder the codification of those practices into international rules. Aside from rule-making at the international fora, it is not unlawful for individual nations to take restrictive measures against particular nations by reasons of the supply chain unless forbidden under international trade law including the WTO legal framework.[122]

[121] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[122] Kadri Kaska, Henrik Beckvard and Tomáš Minárik, 'Huawei, 5G and China as a Security Threat,' NATO CCDCOE, March 2019, p. 13, https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf; Giovanna Adinolfi, 'States' Measures to Counter Cyberattacks from the Perspective of International Economic Law,' in François Delerue and Aude Géry, ed., with contributions from Giovanna Adinolfi, Talita Dias, Duncan B. Hollis, Vera Rusinova and Barrie Sander, International Law and Cybersecurity Governance, July 2022, pp. 19-30, https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/fQBr45KY/international-law-and-cybersecurity-governance.pdf

6. Conclusions

There are no international legally binding rules or principles in the field of cybersecurity of the supply chain and a growing number of states perceive a need for national frameworks and mechanisms and for globally common rules for that purpose, as shown in some discussions ongoing at the UN. Western countries have developed some frameworks at the regional and national levels based on their commonly shared perception that the supply chain can be vulnerable to threats from adversarial foreign countries. From the overview of national regulative measures in the four countries reviewed by this paper, the commonalities are shown in Table 1.

Table 1: Comparison of National Approaches

	Finland	Japan	UK	US
Legally regulated at the domestic level?	○	△(1)	○	○
All Items/contracts covered in MOD/DOD?	△(2)	○(3)	○(4)	○(5)
Listing of specific country's products in regulations?	×	×	○ China	○ Russia China
Excluding (or not acquiring) of specific country's products in practice?	○	○	○	○

Symbols

○: well-regulated, △: partially regulated, ×: not regulated

Notes

(1) Understanding between Ministries plus local regulation in each organisation.

(2) The most critical parts of the communication network are covered.

(3) All new contracts on information technologies products and services.

(4) All new contracts involving the electronic exchange of MOD Identifiable Information (See the definition in note 62).

(5) All contracts involving designated vendors.

Despite a lack of binding agreements, all four countries reviewed in this paper have domestic legislation or documents to regulate the supply chain to safeguard national security and foreign policy interests. All except Japan have legislation on this matter and all but Finland appear more comprehensive in covering almost all products and services, at least according to the publicly available information. Finland's regulations appear more limited in scope, as they only focus on 'the most critical parts of the communication network.'

The UK and US are explicit in targeting particular high-risk vendors such as Huawei and particular countries such as China or Russia and strict requirements are imposed on domestic providers to remove these high-risk vendors from their networks. Finland and Japan are not so specific. However, all four have come to a similar practice by excluding or refraining from acquiring certain products and services made by certain countries.

National practices on the cybersecurity of the supply chain and the threat perceptions behind these practices such as which state or phenomenon constitutes the threat vary between countries, even between EU and NATO countries. Thus, it is even more difficult to develop common rules and standards at the international level. However, there is a pressing need to address the threats ahead of actual incidents since no country is exempt from supply chain cyberattacks. Therefore, further exchange of good practices across a wide range of countries as recommended by the UN GGE 2021 Report (para. 57 (b)) could be the best way ahead. Transparency, objectivity, and impartiality of these national approaches are key to success, as proposed in the UN GGE Report (para. 57 (a)).

7. References

Adinolfi, Giovanna, 'States' Measures to Counter Cyberattacks from the Perspective of International Economic Law,' in François Delerue and Aude Géry, ed., with contributions from Giovanna Adinolfi, Talita Dias, Duncan B. Hollis, Vera Rusinova and Barrie Sander, International Law and Cybersecurity Governance, July 2022. https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/fQBr45KY/international-law-and-cybersecurity-governance.pdf

Alkio, Mikko and Rouvinen, Petri, 'Implementing the 5G Toolbox: Could Finland Serve as a Model for the Other EU Countries?,' Avance Insight, January 2021. https://www.avance.com/wp-content/uploads/2021/05/AVANCE-Insight-01-2021.pdf

Bermingham, Finbarr, 'Huawei 5G Ban is Upheld by Swedish Court in Further Blow to Chinese Telecoms Giant's European plans,' South China Morning Post, 23 June 2021. https://www.scmp.com/news/china/article/3138369/huawei-5g-ban-upheld-swedish-court-further-blow-chinese-telecoms-giants

Council of the European Union, 'Council Conclusions on ICT Supply Chain Security,' Approved by the Council at its Meeting on 17 October 2022, 13664/22. https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf

Demidov, Oleg and Paoli, Giacomo Persi 'Supply Chain Security in the Cyber Age, UNIDIR, 2020. https://unidir.org/sites/default/files/2020-02/Supply%20Chain%20Security%20in%20the%20Cyber%20Age%20-%20UNIDIR%20Report.pdf

ENISA, 'Ad-Hoc Working Group 03 - on 5G Cybersecurity Certification,' 25 October 2021. https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification ,

ENISA, 'Call for Applications for the ad hoc Working Group on the Preparation of a Candidate EU 5G Cybersecurity Certification Scheme,' June 2021. https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification/ad-hoc-working-group-on-5g-cybersecurity-certification

ENISA, 'EU Cybersecurity Certification – FAQ.' https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq/certification-schemes-and-cabs-faq

ENISA, 'Securing EU's Vision on 5G: Cybersecurity Certification,' 3 February 2021. https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

ENISA, 'Threat Landscape for Supply Chain Attacks,' July 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

'EU Nations Divided on 5G Security, Auditors Say,' Euractiv, 8 January 2021. https://www.euractiv.com/section/5g/news/eu-nations-divided-on-5g-security-auditors-say/

European Commission, 'Cyber Resilience Act, ' 15 September 2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

European Commission, 'Cybersecurity of 5G Networks - EU Toolbox of Risk Mitigating Measures,' 29 January 2020. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

European Commission, 'Member States Publish a Report on EU Coordinated Risk Assessment of 5G Networks Security,' 9 October 2019. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049

European Commission, 'Proposal for Directive on Measures for High Common Level of Cybersecurity Across the Union,' 16 December 2020. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

European Commission, 'Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity,' 24 July 2020. https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

European Commission, 'Security of 5G Networks: EU Member States Complete National Risk Assessments,' 19 July 2019. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_4266

European Commission, 'Shaping Europe's Digital Future,' European Commission, 26 March 2019. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks

European Parliament, Resolution of 12 March 2019 on Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them (2019/2575(RSP)). https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html

European Parliament, 'Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them,' 12 March 2019. https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1577382&l=en&t=D

'Finnish Parliament Passes Law to Allow Banning Telecoms Equipment on Security Grounds,' Telecompaper, 9 December 2020. https://www.telecompaper.com/news/finnish-parliament-passes-law-to-allow-banning-telecoms-equipment-on-security-grounds-2--1364991

Gallagher,' Jill C., U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy and Economic Interests,' Congressional Research Service, R47012, 5 January 2022. https://www.everycrsreport.com/files/2022-01-05_R47012_65c5c54827b8fef912a19079f10e144b3b88d009.pdf

'Huawei Challenges Legality of 5G Bans in Poland, Romania,' Politico, 2 November 2020. https://www.politico.eu/article/huawei-hints-at-legal-action-against-5g-bans-in-poland-romania/

'Huawei Appeals Sweden's 5G Equipment Ban,' 5G Observatory, 2 October 2021. https://5gobservatory.eu/huawei-appeals-swedens-5g-equipment-ban/

'Huawei is Taking Sweden to Court After the Country Banned its 5G products,' Euronews, 31 January 2022. https://www.euronews.com/next/2022/01/31/huawei-is-taking-sweden-to-court-after-the-country-banned-its-5g-products

ICSID, Huawei Technologies Co., Ltd. v. Kingdom of Sweden (ICSID Case No. ARB/22/2). https://icsid.worldbank.org/cases/case-database/case-detail?CaseNo=ARB/22/2

‘Japan Bans Huawei and its Chinese Peers from Government Contracts: Move Aligns with US, Prompting ‘Serious Concerns’ and Protests of ‘Discrimination’,’ Nikkei Asia, 10 December 2018. https://asia.nikkei.com/Economy/Trade-war/Japan-bans-Huawei-and-its-Chinese-peers-from-government-contracts

‘Japan Sets Policy That Will Block Huawei and ZTE from Public Procurement as of April,’ Japan Times, 10 December 2018. https://www.japantimes.co.jp/news/2018/12/10/business/japan-sets-policy-will-block-huawei-zte-public-procurement-april/

Kaska, Kadri, Beckvard, Henrik and Minárik, Tomáš, ‘Huawei, 5G and China as a Security Threat,’ NATO CCDCOE, March 2019. https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf

Kaspersky Lab, ‘Kaspersky Lab’s Corporate Data Protection Technology is FIPS 140-2 Certified,’ 30 November 2016. https://www.kaspersky.com/about/press-releases/2016_kaspersky-lab-s-corporate-data-protection-technology-is-fips-140-2-certified

Layton, Roslyn, ‘Secure Equipment Act Becomes Law,’ Forbes, 1 December 2021. https://www.forbes.com/sites/roslynlayton/2021/12/01/secure-equipment-act-becomes-law/

‘Legislation Barring Huawei 5G tech Passes Riigikogu,’ ERR News, 25 November 2021. https://news.err.ee/1608414737/legislation-barring-huawei-5g-tech-passes-riigikogu

Mulligan, Stephen P and Linebaugh, Chris D, ‘Huawei and U.S. Law,’ Congressional Research Service, R46693, 23 February 2021. https://sgp.fas.org/crs/misc/R46693.pdf

Oertel, Janka, ‘On 5G, Brussels is Up to the Job,’ European Council on Foreign Relations, 3 February 2020. https://ecfr.eu/article/commentary_on_5g_brussels_is_up_to_the_job/

Pernik, Piret, Jančárková, Taťána, Kaska, Kadri, Ruuto, Urmas, Gheorghevici, Costel-Marius and Beckvard, Henrik, ‘Research Report Supply Chain and Network Security for Military 5G Networks,’ NATO CCDCOE, 2021. https://ccdcoe.org/uploads/2021/10/Report_Supply_Chain_and_Network_Security_for_Military_5G_Networks.pdf

‘Romanian President Signs Bill into Law to Ban Huawei from 5G,’ Reuters, 11 June 2021. https://www.reuters.com/business/media-telecom/romanian-president-signs-bill-into-law-ban-huawei-5g-2021-06-11/

‘Swedish Court Upholds Ban on Huawei Sale of 5G Gear,’ Reuters, 22 June 2022. https://www.reuters.com/business/media-telecom/swedish-court-upholds-ban-huawei-sale-5g-gear-2022-06-22/

‘US Bans Huawei from Selling Telecom Gear and Threatens its Supply Chain,’ CNN, 16 May 2019. https://edition.cnn.com/2019/05/15/tech/trump-executive-order-telecom-security/index.html

‘5G-front: Hungary Refuses to Join the Anti-China Coalition,’ Dairy News Hungary, 18 November 2020. https://dailynewshungary.com/hungarian-foreign-ministry-refuses-to-join-the-anti-china-coalition/

UN Doc. A/66/359. https://undocs.org/A/66/359

UN Doc. A/69/723. https://undocs.org/en/A/69/723

UN Doc. A/68/98. https://undocs.org/A/68/98

UN Doc. A/70/174. https://undocs.org/A/70/174

UN Doc. A/76/135. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement

UN Doc. A/AC.290/2021/CRP.2. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

National official documents:

Finland

Ministry of Transport and Communications of Finland, 'Act on Electronic Communications Services Enters Into Force on 1 January 2021,' 30 December 2020. https://valtioneuvosto.fi/en/-/act-on-electronic-communications-services-enters-into-force-on-1-january-2021

Ministry of Transport and Communications of Finland, 'Advisory Board Set Up to Support Network Security.' https://valtioneuvosto.fi/en/-/advisory-board-set-up-to-support-network-security

The Act on Electronic Communication Services (Laki sähköisen viestinnän palveluista), 7.11.2014/917, Finlex. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917 (in Finnish).

`The Government Proposal on the Amendment of the Act (Hallituksen esitys eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi),' Finlex, 11 June 2020. https://www.finlex.fi/fi/esitykset/he/2020/20200098 (in Finnish).

Traficom, `Regulation on Critical Parts of a Communications Network (Viestintä: Määräys viestintäverkon kriittisistä osista),´ TRAFICOM/161584/03.04.05.00/2020, 19 May 2021. https://www.finlex.fi/data/normit/47015/Regulation_on_critical_parts_of_a_communications_network.pdf (Unofficial translation); https://www.finlex.fi/fi/viranomaiset/normi/480001/47015 (in Finnish).

Japan

METI, 'Cabinet Decision on the Bill for the Act on Promotion of Developing/Supplying and Introducing Systems Making Use of Specified Advanced Information Communication Technologies (「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律」),' 18 February 2020. https://www.meti.go.jp/english/press/2020/0218_001.html; See the Act, https://elaws.e-gov.go.jp/document?lawid=502AC0000000037 (in Japanese).

METI, Press Conference by Minister Seko (excerpted version. provisional translation), 14 December 2018. https://www.meti.go.jp/english/speeches/press_conferences/2018/1214001.html

MIC, ed., White Paper: Information and Communication in Japan (『情報通信白書令和２年版』), 2020. https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2020/chapter-3.pdf (in English); https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/n3400000.pdf (in Japanese)

MIC, 'Approval of Plans on Setting Up of 5G Specific Base Stations,' April 2019. https://www.soumu.go.jp/main_content/000613734.pdf (in Japanese).

MOD, 'General Notice by the Commissioner of the Acquisition, Technology & Logistics Agency (ATLA) of Japan MOD, on Measures for Addressing Supply Chain Risks involving Procurement of Information Technology (IT) assisted Defense Equipments and Associated Services (防衛装備庁長官「IT 利用装備品等及び IT 利用装備品等関連役務の調達におけるサプライチェーン・リスクへの対応につ

いて（通知）」),' 21 January 2021, last amended on 31 March 2021. https://www.mod.go.jp/j/procurement/seido/buppin_ekimu/pdf/zenpan_04.pdf (in Japanese).

MOD, 'General Notice by the Commissioner of the ATLA of Japan MOD, on Details of Measures for Addressing Supply Chain Risks Involving Procurement of Information Systems (防衛装備庁長官「情報システムに関する調達に係るサプライチェーン・リスク対応のための措置の細部事項について（通知）」),' 9 January 2019, last amended on 31 March 2021. http://www.clearing.mod.go.jp/kunrei_web/ (in Japanese).

MOD, 'Notice by the Vice-Minister of Defense, on Measures for Addressing Supply Chain Risks Involving Procurement of Information Systems (防衛事務次官「情報システムに関する調達に係るサプライチェーン・リスク対応のための措置について（通達）」),' 31 January 2019, last amended on 29 March 2019. https://www.mod.go.jp/gsdf/tercom/img/file503.pdf (in Japanese).

NISC, 30th meeting of the CSSH, Material 8 `Amendment of the Understanding,´ 7 July 2021. https://www.nisc.go.jp/conference/cs/dai30/pdf/30shiryou08.pdf (in Japanese).

NISC, 'Understanding (Agreement) on Government Procurement Policy and Procurement Procedures for IT Goods and Services (「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」),' 10 December 2018, last amended 2021. https://www.nisc.go.jp/active/general/pdf/choutatsu_moushiawase0901.pdf (in Japanese).

The Act on General Rules for Incorporated Administrative Agencies (「独立行政法人通則法」), Act No. 103 of 1999, as amended as Act No. 66 of 2014, Japanese Law Translation Database System. https://www.japaneselawtranslation.go.jp/ja/laws/view/2754#je_ch1sc1at2

The Basic Act on Cybersecurity (「サイバーセキュリティ基本法」), Act No. 104 of 2014, Japanese Law Translation Database System. https://www.japaneselawtranslation.go.jp/en/laws/view/3677

The Minute of Committee of National Security of the House of Representatives; Answer by a MOD senior official Mr. Hideki Tsuchimoto (土本政府参考人), 208th Session of the National Diet, 3 June 2022. https://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/001520820220603007.htm (in Japanese).

The United Kingdom

Cabinet Office, Procurement Policy Note – Cyber Essentials Scheme. ACTION NOTE 09/14, 25 MAY 2016. https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification

'DCPP Cyber Security Model: Industry Buyer and Supplier Guide,' 30 March 2017, last updated 22 June 2018. https://www.gov.uk/government/publications/dcpp-cyber-security-model-industry-buyer-and-supplier-guide

Explanatory Note: Telecommunications (Security) Act 2021. https://www.legislation.gov.uk/ukpga/2021/31/notes/contents

'Foreign Secretary's Statement on Huawei,' 28 January 2020. https://www.gov.uk/government/speeches/foreign-secretary-statement-on-huawei

'Huawei to be Removed from UK 5G Networks by 2027,' 14 July 2020. https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027

MOD, 'Guidance: Cyber DEFCON 658,' 10 September 2021. https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down/cyber-defcon-658#definitions-1

MOD, 'Guidance: DCPP: Your Questions Answered,' 26 October 2017. https://www.gov.uk/government/publications/defence-cyber-protection-partnership-your-questions-answered/dcpp-your-questions-answered-html

MOD, 'Guidance Cyber Security for Defence Suppliers (Def Stan 05-138),' 17 October 2017, updated 1 July 2021. https://www.gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138

MOD, 'Guidance Cyber Security Model: Cyber Risk Profiles' Requirements,' 24 March 2015, updated 24 July 2020. https://www.gov.uk/government/publications/defence-cyber-protection-partnership-cyber-risk-profiles

NCSC, 'About Cyber Essentials.' https://www.ncsc.gov.uk/cyberessentials/overview

NCSC, 'NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks,' 28 January 2020. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

NCSC, 'Summary of the NCSC Analysis of May 2020 US Sanction,' NCSC, 14 July 2020. https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction

NCSC, 'Supply chain security guidance,' 28 January 2018. https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

'Policy Paper: Government Response to the Call for Views on Supply Chain Cyber Security,' 15 November 2021. https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security/government-response-to-the-call-for-views-on-supply-chain-cyber-security

'Policy Paper: Telecommunications (Security) Bill: Illustrative Designated Vendor Direction and Designation Notice,' 30 November 2020. https://www.gov.uk/government/publications/telecommunications-security-bill-illustrative-designated-vendor-direction-and-designation-notice

[final version] 'Designation Notice under section 105Z8 of the Communications Act 2003 Designating Huawei for the Purposes of a Designated Vendor Direction,' 12 October 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1110247/Final_Huawei_Designation_Notice.pdf

Secretary of State for Digital, Culture, Media and Sport, 'UK Telecoms Supply Chain Review Report,' July 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

The National Cyber Security Strategy 2016 to 2021, 2016. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, November 2011, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

The United States

Bureau of Industry and Security (BIS) of the US Department of Commerce, Addition of Entities to the Entity List, Federal Register, Vol. 84, 21 May 2019. https://www.govinfo.gov/content/pkg/FR-2019-05-21/pdf/2019-10616.pdf

Code of Federal Regulations Title 47, § 1.50002 Covered List. https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-1/subpart-DD/section-1.50002

Department of Commerce, 'ICT Supply Chain: Securing the Information and Communications Technology and Services Supply Chain.' https://www.commerce.gov/issues/ict-supply-chain#:~:text=14034)%2C%20on%20November%2023%2C,2021%20(86%20FR%204909).

Department of Commerce, 'ICT Supply Chain.' https://www.commerce.gov/issues/ict-supply-chain

Department of Justice, 'Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud,' 28 January 2019. https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial

Department of Justice, press release, 'Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies,' 15 May 2020. https://2017-2021.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts.html

Executive Order 13873 of 15 May 2019 on Securing the Information and Communications Technology and Services Supply Chain, Federal Register, Vol. 84, 17 May 2019. https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

DoD, 'Open FAR Cases as of 3/24/2023.' https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf

Executive Order 14034 of 9 June 2021 on Protecting Americans' Sensitive Data From Foreign Adversaries, Federal Register, Vol. 86, 11 June 2021. https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries

FCC, First Report and Order, Order and Further Notice of Proposed Rulemaking, adopted on 22 November 2019, WC Docket No. 18-89, PS Docket Nos. 19-351, 19-352, 34 FCC Rcd 11423 (14). https://www.fcc.gov/document/protecting-national-security-through-fcc-programs-0

FCC, List of Equipment and Services Covered By Section 2 of The Secure Networks Act. https://www.fcc.gov/supplychain/coveredlist

FCC, 'Notice of Proposed Rulemaking: Protecting Against National Security Treats to the Communications Supply Chain Through FCC Programs,' 18 April 2018. https://www.fcc.gov/document/fcc-proposes-protect-national-security-through-fcc-programs-0

FCC, 'Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs.' https://www.fcc.gov/supplychain

FCC, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, Federal Register, Vol. 86, 6 October 2021. https://www.govinfo.gov/content/pkg/FR-2021-10-06/pdf/2021-21783.pdf.

FCC, Public Notice, 'Public Safety and Homeland Security Bureau Issues Final Designations of Huawei Technologies Company and ZTE Corporation as Companies Posing a National Security Threat to the Integrity of Communications Networks and the Communications Supply Chain,' PS Docket Nos. 19-351, 19-352. https://www.fcc.gov/document/fcc-designates-huawei-national-security-threat

Federal Register, Vol. 86, 17 May 2021. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

Huawei Technologies v. FCC & USA on Petition for Review of an Order of the FCC, No. 19-60896, US Court of Appeals for the Fifth Circuit, 18 June 2021. https://docs.fcc.gov/public/attachments/DOC-373457A1.pdf

Kaspersky Lab, Inc. et al v. Department of Homeland Security et al, US Court of Appeals for the District of Columbia Circuit, Nos. 1:17-cv-17-2697 and 1:18-cv-325, 909 F.3d 446, 453-64 (D.C. Cir. 2018). https://cases.justia.com/federal/appellate-courts/cadc/18-5176/18-5176-2018-11-30.pdf?ts=1543591852

Memorandum Opinion and Order, Huawei Technologies USA, Inc., et al. v. The United States of America, et al., 13, U.S. District Court for the Eastern District of Texas, No. 4:2019-cv-00159 - Document 51 (E.D. Tex. 2020). https://law.justia.com/cases/federal/district-courts/texas/txedce/4:2019cv00159/188186/51/

NIST, 'Fact Sheet: Executive Order on Improving the Nation's Cybersecurity,' May 2022. https://www.nist.gov/system/files/documents/2022/05/24/EO%20Fact%20Sheet.pdf

The archived US Department of State website, 'Secretary Michael R. Pompeo At a Press Availability: Remarks to the Press,' 29 April 2020. https://2017-2021.state.gov/secretary-michael-r-pompeo-at-a-press-availability-4/index.html

The archived US Department of State website, 'Under Secretary Keith Krach Remarks on U.S.-Eswatini Clean Network Declaration,' 15 January 2021. https://2017-2021.state.gov/under-secretary-keith-krach-remarks-on-u-s-eswatini-clean-network-declaration/index.html

The archived US Department of State website, 'United States – Slovak Republic Joint Declaration on 5G Security,' 23 October 2020. https://2017-2021.state.gov/united-states-slovak-republic-joint-declaration-on-5g-security/index.html

The Law Library of US Congress, Public Law No. 115-91, Section 1656 [Security of nuclear command, control and communications system from commercial dependencies]. https://www.congress.gov/bill/115th-congress/house-bill/2810/text

The Law Library of US Congress, Public Law No. 115-232, Section 889 [Prohibition on certain telecommunications and video surveillance services or equipment]. https://www.congress.gov/bill/115th-congress/house-bill/5515/text

The Law Library of US Congress, Public Law No. 116-124. https://www.congress.gov/bill/116th-congress/house-bill/4998/text

The Law Library of US Congress, Public Law No. 117-55. https://www.congress.gov/117/plaws/publ55/PLAW-117publ55.pdf

The Law Library of US Congress, Report of the House Committee on Energy and Commerce, 19 October 2021. https://www.congress.gov/congressional-report/117th-congress/house-report/148/1

The United States Code, Title 47, Sections 201 (b), U.S. Government Publishing Office. https://www.govinfo.gov/content/pkg/USCODE-2021-title47/pdf/USCODE-2021-title47-chap5-subchapII-partI-sec201.pdf#:~:text=(b)%20All%20charges%2C%20practices,communications%20by%20wire%20or%20radio

The US Embassy and Consulate in Greece, `The Transatlantic Alliance Goes Clean.´ https://gr.usembassy.gov/the-transatlantic-alliance-goes-clean/

White House, 'Executive Order on Improving the Nation's Cybersecurity,' 12 May 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/