Telecommunications Policy 45 (2021) 102216

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol

European Union policy on 5G: Context, scope and limits☆

Margarita Robles-Carrillo

Network Engineering & Security Group (NESG), University of Granada, Spain

ARTICLE INFO

Keywords:
5G
European Union
Member states
Policies

ABSTRACT

5G is considered a key technology for society but its implementation is currently surrounded by controversy. Beyond its technical aspects, 5G has become a question of security and national interest for many States as well as an international policy issue. Technological autonomy and digital sovereignty are increasingly recognised as strategic priorities on a global scale. In this context, the EU's position is unique, basically for two reasons. On the one hand, the EU has unintentionally become part of the playing field in the US-China dispute over technology companies and 5G. On the other hand, any policy of the EU or its Member States is constrained by the nature of 5G as an area of either European or national competence. The delimitation of their competences is not clear, just as there is no transparent and understandable distinction of their 5G responsibilities. In order to clarify this situation, a comprehensive analysis of the European competence and legal frameworks is necessary. After that, the study of the evolution process of this European policy provides an overview of its scope and limits. Finally, the paper explains the procedures and instruments of this European policy and concludes by assessing its implementation and development prospects. The possibility of reaching technological autonomy and digital sovereignty for the EU and its member states depends, for the time being, on this European policy.

1. Introduction

For some time now, 5G technology has been at the centre of controversy. In the last few years, the scientific and technological debate concerning its different applications or implementation modalities, benefits or risks, has been somewhat sidestepped in the public sphere by disputes of a different nature, mainly, trade wars (Houser, 2020, p. 549) (Alfayad, 2029, p. 47) (Mascitelli and Chung, 2021),[1] cyber espionage allegations (Kaska et al., 2019, p. 10) (Rühlig & Björk, 2020, , p. 4)[2], threats of sanctions (CSR, 2020) (Balding, 2019), or

☆ * Work partially supported by Spanish Government through Project PID 2020-114495RB-I00 and by Network Engineering & Security Group (NESG).

E-mail address: mrobles@ugr.es.

[1] The Trump Administration has started a trade war against China that was considered its boldest move in the context of its global foreign policy. After the adoption of safeguard tariffs on Chinese imports in 2018, "the conflict was further fueled by US concerns that the Chinese government could force domestic companies such as Huawei, the market leader for 5G technology, to install backdoors for espionage" (Janusch & Lorberg, 2020, p. 94).

[2] Shoebridge explains that "Russia has had a higher profile, but China has been the giant of cyber espionage … Beyond government, China has engaged in the cyber-enabled theft of intellectual property, trade secrets, and commercial-in-confidence material from multiple companies internationally – as reporting in the US has clearly demonstrated over the past few years. Coupled with this demonstrated intent to conduct wide-ranging cyber espionage, China's intelligence law provides the capability to compel Huawei to assist with state intelligence efforts. Article 7 of China's 2017 Intelligence Law obliges organizations and citizens to support, assist, and cooperate with intelligence work" (Shoebridge, 2018, p. 2) (CSR, 2020) (Rühlig & Björk, 2020, p. 9). On the other side, Cartwright argues that "the United States has been able to exploit the international market dominance of US-based internet companies in order to internationalize State power through surveillance programmes conducted by national security and law enforcement agencies" (Cartwright, 2020, p. 1).

https://doi.org/10.1016/j.telpol.2021.102216
Received 30 March 2021; Received in revised form 7 July 2021; Accepted 7 July 2021
Available online 27 July 2021

disinformation practices (Meese et al., 2020), among others. To some extent, for different and quite unjustified reasons, unconnected to its technical component, 5G is also being associated with negative perceptions, images or narratives.

For some time now, furthermore, the public debate on 5G has not been focused on the meaningful economic, social and political dimensions and consequences of this technology. This debate has not really been addressed accurately. Most of these controversies -trade war, sanctions, bans or restrictive measures-are not the main issues but rather evidence of the root problem: the technological dependence on foreign States or external providers and the value of strategic autonomy and digital sovereignty.

The question of technology dependence, that has been emerged for quite some time,[3] is now becoming even more relevant mainly for two reasons: on the one hand, the global reach and implications of 5G technology for the economy, society and politics as a whole; and, on the other, the fact that it is the first time during the Internet era that Chinese companies enjoy technological and commercial leadership (Erie & Streinz, 2021, p. 30). In recent years, China's economic, commercial and technological power has been growing steadily. As Eric and Streinz explain, "Chinese technology companies increasingly supply the relevant physical components of digital infrastructures, set the relevant standards (both domestically and internationally), and operate and control digital platform infrastructures outside China" (Erie & Streinz, 2021, pp. 31–32).[4] Mascitelly and Chung recognise that "there were few cases in history where countries emerge economically with such gusto and haste as has China. Certainly not in modern industrial times has one single country come from such a low economic base to be declared as a global superpower and even threatening the position of the United States in such a short time span" (Mascitelli and Chung, 2021:1).

Bearing this situation in mind, in some way, "5G rollout needs to be recognised as a strategic rather than merely a technological choice" (Kaska et al., 2019, p. 20). There is also a debate as to whether technological power[5] may be taking the place that military power has traditionally held from a political and security perspective (CSR, 2020) (Inkster, 2019, p. 105) (Kaska et al., 2019, p. 5) (Canosa & Fiore, 2019, p. 182).[6] Many States are currently addressing 5G not only in terms of cybersecurity but also in terms of national security or national interest.[7] From a legal and political point of view, this is a major paradigm shift.[8]

The United States (US) has been at the centre of this controversy, placing Chinese companies among the targets of its national security policy (CSR, 2020) (Schaefer, 2020, p. 1501) (Janusch & Lorberg, 2020, p. 94) (Balding, 2019).[9] At home, the US has taken a succession of measures aimed at limiting their activities as service providers (Alfayad, 2029: 47), while in its foreign policy it has demanded of its allies, mainly, but not only European countries (Mascitelli and Chung, 2021), their adhesion to American guidelines. The arrival of Biden to the US Presidency has not involved a major shift concerning Chinese companies. However, there has been a significant change in US relations with European countries and the EU. The aim is to increase cooperation with Europe in a more conciliatory discourse, but still aimed at neutralising China[10]. China has also put pressure on European countries in order to protect its own interests (Rühlig & Björk, 2020, p. 5). European States have reacted differently to this situation (Drahokoupil et al., 2017, p. 211). For a long time, there has been no uniform joint policy or reaction at the European Union (EU) level.

Besides being an international organization, the position of the EU concerning this technology is particularly complicated because

[3] Lysne et al. argue that "Complexities in the digital value chains constitute a paradox; you cannot trust anyone, yet you have no choice, but to trust everyone.1 A nation State can never fully trust the electronic equipment that resides in its critical infrastructures. The existence of untrusted electronics must therefore either find its solution in architecture of infrastructures, or in political trust through international relations and alliances" (Lysne et al., 2019, p. 1).

[4] For the authors, "If Chinese technology companies build equipment according to a certain standard and export this equipment to other countries, the standards embedded in the products get exported as well. This basic insight is true not only for cellular networks and their technical standards; it also applies to other digital infrastructures" (Erie & Streinz, 2021, p. 30).

[5] Cartwright defends that "As Chinese companies become more competitive, they threaten both the commercial dominance of US companies as well as the geopolitical power of the US state" (Cartwright, 2020, p. 1). The Chinese companies also exemplify new economic and commercial dynamics (Fu et al., 2018, p. 202).

[6] Yun Wen argues "that the rise of Huawei was closely tied to the turns and twists of China's digital revolution. It came to symbolize a continuity of China's nation-centric developmental strategy and the legacies of self-reliant development on the one hand, and was enmeshed with the country's aspirations of reintegration into transnational digital capitalism on the other. The company's strategy of internationalization, in conjunction with the Chinese state's outward expansion, illustrates a peculiar logic, pattern and ramification of Chinese capital's outward expansion. By investigating the dynamics and contradictions of Huawei's capital accumulation, this dissertation also foregrounds the geoeconomic and geopolitical tensions arising from the globalization of China's corporate power. This case suggests a potential realignment of the global political economic order" (Wen, 2017).

[7] https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

[8] Ly and Ly refer to 5G as an important catalytic factor (Li & Li, 2021: 92).

[9] Alongside with Huawei, TikTok and other Chinese companies have also been included among the targets of restrictive measures (Medina Serrano et al., 2020, p. 6) (CSR, 2020).

[10] On 15 June 2021, at the end of the Summit 2021, the EU and the US have adopted the Statement "Towards a renewed Transatlantic partnership" with the aim "to drive digital transformation that spurs trade and investment, strengthens our technological and industrial leadership, boosts innovation and protects and promotes critical and emerging technologies and infrastructure". EU and US have decided to cooperate on the development and deployment of new technologies "based on our shared democratic values, including respect for human rights, and that encourages compatible standards and regulations". This cooperation includes a high-level EU-US Trade and Technology Council (TTC). (https://www.consilium.europa.eu/media/50758/eu-us-summit-joint-statement-15-june-final-final.pdf).

5G is a novel area of competence. As such it is not assigned to a single authority, but rather involves the competences of the Union on the one hand, and those of its Member States on the other. While Member States have started to adopt measures based on national interest or security grounds,[11] the EU has recognised that the security of 5G networks is a matter of strategic importance which requires a common European approach.

From a legal point of view, European States have no freedom of action and, when they act, they have to respect the EU competences. The EU has no specific power for 5G and has also to respect national powers. As a system with competences divided and shared between the Union and its Member States, each of them must act within the limits of its own competences and with respect for the competences of the others. Notwithstanding this complex network of competences, the EU and its Member States have been taking different measures concerning 5G (Mascitelli and Chung, 2021) (Lysne et al., 2019, p. 3). Then, an additional and no less significant problem arises, namely that it is not always easy to fully understand who is taking the measures and why they are being taken. And most importantly, who has the ultimate responsibility for 5G policy.

By addressing these issues from a legal perspective, the aim of this paper is to analyze 5G policy in the European Union in order to determine its scope, content and limits in the context of this political-strategic challenge. There are three interrelated questions to answer. The first is whether and how to guarantee strategic autonomy and digital sovereignty for Europeans and in an organisational model such as the EU. Although there is no legal or even political definition of the concepts of digital autonomy and strategic sovereignty, both have become the benchmarks for Europe's digital transformation in different sectors, including 5G. The second question is how to organize the competences of the EU and the States, taking into account the multifaceted issues raised by 5G. The third is how to explain this model clearly and openly. The European 5G model needs to be understood and transparency and accountability needs to be ensured.[12]

To this end, in this paper, Section 2 explains the current debate on 5G with the purpose of identifying the different aspects of the issues raised by this technology from a legal-political perspective. After that, Section 3 analyses the competence and legal frameworks where the juridical basis for European action can be found and to what extent. On that basis, Section 4 is dedicated to the process of development of this European policy approach. Section 5 identifies and analyses its two main instruments: the EU Coordinated Risk Assessment of the Cybersecurity of 5G networks and the EU Toolbox on 5G Cybersecurity. Section 6 serves to evaluate their implementation and the perspectives opened for the evolution of this EU policy. In the course of the paper and in the conclusions included in Section 7, the three questions raised on digital sovereignty, the organization of competences and the need for transparency and accountability of the European 5G model are answered as much as possible from a legal point of view.

2. Scope and nature of the 5G debate

Security in 5G networks has become a polyhedric problem that seems to go beyond its natural object and scope, which is essentially technological, to reveal itself as a matter of policy, strategy and international security (Wen, 2017).[13]

On the *technical* side, the advantages of this technology include higher speeds and greater capacity, latency, reliability, flexibility and efficiency (I. et al., 2014: 66) (Akyildiz, Nie, Lin, & Chandrasekaran, 2016) (Rost et al., 2016).[14] But it is also associated with significant threats and risks (Cave, 2018) (Khan et al., 2020, p. 196). The literature has warned about the main vulnerabilities and challenges of this technology (Andrews et al., 2014, p. 1065) (Boccardi et al., 2014, p. 74) (Cai et al., 2018), as well as the need for innovative 5G security solutions (Gupta & Jha, 2015) (Hussain et al., 2019) (Gil Pérez 2017, pp. 59–65, p. 59) (Navarro-Ortiz et al., 2020, p. 905) (Ahmad et al., 2019, p. 3682). Studies conducted by ENISA, the ITU and ICANN provide a scenario for 5G that is both exciting and worrying (ENISA, 2019).[15] However, 5G is not only a new paradigm for electronic communications.[16]

On the *socio-economic and political* sides, 5G has been defined as the essential technological component in the digital transformation of society and the economy in the most advanced countries over the next decade (Campbell et al., 2017, pp. 1–35) (Rao & Prasad, 2018) (Matinmikko et al., 2018).[17] By contrast to the replacement of 3G by 4G, 5G is widely recognised as having a cross-cutting effect

[11] About the situation of Huawei in Europe, see Drahokoupil et al., 2017, pp. 211–229.

[12] Following to the Prague Proposals, "Laws and policies governing networks and connectivity services should be guided by the principles of transparency and equitability, taking into account the global economy and interoperable rules, with sufficient oversight and respect for the rule of law" (https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/).

[13] At the Prague 5G Security Conference held in May 2019, bringing together 32 countries from Europe and North America, the Prague Proposals include the principle that 5G is not only a technical issue (https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/).

[14] https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx.

[15] ENISA. Threat Landscape for 5G Networks, 2019 (https://www.enisa.europa.eu/news/enisa-news/enisa-draws-threat-landscape-of-5g-networks); ITU (2020). 5G - Fifth generation of mobile technologies (https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx); ICANN (2020).

[16] Agiwal et al. explain the paradigm shift of 5G architecture takin into account its different components (Agiwald, Roy, & Saxena, 2016, pp. 1620–1625).

[17] That includes the question of sustainability as a main goal of the United Nations (West, 2016).

on the economy and society as a whole (Andrews et al., 2014) (Ministry of Energy, Tourism and Digital Agenda, 2018).[18] It is consequently much more than a technological issue (Kaska et al., 2019, pp. 1–26, p. 6). Not surprisingly, for some time now, 5G has been at the centre of the international economic and political debate (Dominioni and Rugge, 2020, pp. 1–23).

On a *strategic and security* perspective, 5G seems to be currently the most obvious and pervasive evidence of the challenges posed by the technological dependence of States.[19] According to the Prague Proposals, a set of recommendations issued from the Prague 5G Security Conference, "security of 5G networks is crucial for national security, economic security and other national interests and global stability"[20]. Identifying an issue as a problem of national interest or national security has greater consequences than would initially be expected.[21] Indeed, a securitization theory was developed by the Copenhagen School in the 1990s (Stritzel, 2014, pp. 11–37). According to this theory, securitization has been defined as the discursive process through which an intersubjective understanding is constructed within a political community to treat something as an existential threat, justifying for urgent and exceptional measures to deal with it. There are two main consequences when a particular issue is securitized: first, it becomes prioritized as regards "normal politics"; and second, "extraordinary means" are necessary and justified to address the problem (Mackenzie, 2010, p. 204).

At first, the debate on 5G in terms of national interest and security has been largely monopolised by the discourse of the Trump Administration against certain companies linked to China (Houser, 2020, p. 549) (Mascitelli and Chung, 2021) (Brake, 2018, pp. 1–30). Huawei has been one of the priority targets of the US Administration's restrictive actions (Yan and Huang, 2020, pp. 1–11), (Noble, Mutimear, & Vary, 2019, pp. 35–40) (Rühlig & Björk, 2020, p. 16).[22] Other Chinese companies have also been targeted with protectionist measures (Schaefer, 2020, p. 1502) (Murmann, 2020). Such actions have been seen as an offensive use of so-called lawfare by the US against China(Mascitelli and Chung, 2021) or the result of China's technology ambitions (Inkster, 2019).[23] However, the underlying component of the trade war and cyber espionage allegations (Houser, 2020, p. 549) (Shoebridge, 2018, p. 1), which intermittently flares up between these States, is not enough to explain the relevance that 5G networks have acquired in their political and strategic discourse.

In 2019, the US National Defence Authorisation Act excludes technology developed by foreign companies from defence equipment (Balding, 2019; US, 2019).[24] In March 2020, the National Strategy to Secure 5G qualifies the issue as a national security problem (CRS, 2020; US, 2020).[25] In January 2021, the US Administration adopts the National Strategy to Secure 5G Implementation Plan that will be managed under the leadership of the National Security Council and the National Economic Council, supported by the National Telecommunications and Information Administration (NTIA) (US, 2021a).[26] Its Line of Effort Four is devoted to "Promote Responsible Global Development and Deployment of 5G". That includes, among others things, to encouraging US leadership in international standards development for 5G, including through private sector and international engagement. The protection of the national interest is therefore not limited to US territory, but justifies a foreign policy aimed at asserting US international leadership in 5G.

The doctrine has considered the adoption of those measures against foreign companies as a possible contravention of the rules of the World Trade Organization (Mascitelli and Chung, 2021). On the other side, the subsidies granted by the Chinese government to Chinese companies have been questioned on the grounds that they constitute a violation of the competition rules (Canosa & Fiore, 2019: 185). In the end, the use of technology companies in the international geopolitical game has become a common practice

[18] According to the Fondation Concorde, in contrast to its predecessors, 5G is a revolution (Fondation Fondation Concorde, 2017: 4). For 5G Americas, "5G, or "Fifth Generation" mobile wireless technologies, are projected to be a disruptive force central to the development of the Fourth Industrial Revolution (5G Americas, 2020).

[19] Alon et al. explain that "Huawei brings two non-Western world powers, China and Russia, closer at a time when these two countries are diverging from global standards of democracy and freedom. Huawei chose Russia as the first country for international expansion in 1997, when Russia was facing an economic crisis (…). China's economic might married with Russia's military one can wreck great havoc in case of a worldwide conflict" (Alon et al., 2021, p. 2).

[20] https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

[21] Kaska et al. argues that "The issue of Huawei technology and 5G represents classic dilemmas inherent to cybersecurity: the impact of stimulating the economy to national security and vice versa, and of modernizing infrastructure to critical infrastructure protection (and vice versa). Given the significance of backbone national infrastructure, defining a position on these dilemmas is a far more complex challenge than simply finding an acceptable balance on a linear scale: it entails comprehensive understanding of all risks, socioeconomic and security, and mitigating those that are critical by means that are available, i.e. that the society can afford" (Kaska et al., 2019, p. 19).

[22] Alon et al. consider that: "Clearly, Huawei is one of the key components of China's geopolitical playbook for global dominance. Countries under the US sphere of influence, and those rivalling nations, such as India, have selectively restricted the development of Huawei" (Alon et al., 2021, p. 2) (Quintana, 2021).

[23] Mascitelly and Chung explain the rise of China as a global power (Mascitelly and Chung, 2021).

[24] https://www.congress.gov/115/crpt/hrpt676/CRPT-115hrpt676.pdf.

[25] https://www.ntia.doc.gov/files/ntia/publications/booz_allen_hamilton-06252020.pdf.

[26] https://www.ntia.gov/files/ntia/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final.pdf.

(Cartwright, 2020, p. 3) (Kaska et al., 2019, p. 12). Moreover, the adoption of measures based on the national interest or national security may justify the recourse to the security exception of the Article XXI of the Marrakesh Agreement (Kaska et al., 2019, , p. 13).[27] The Biden Administration has changed the form[28] but not the substance.[29] In February 2021, the President adopts a new Executive Order on America's Supply Chains (US, 2021b)[30].

In this climate of tension, diplomatic action has even become unusually aggressive (Mascitelli and Chung, 2021).[31] Whether for political affinity, security reasons or other reasons, several countries have adopted protectionist policies (Shoebridge, 2018).[32] The United Kingdom, Germany, Italy or France have entered into this dynamic (Rühlig & Björk, 2020), as well as other non-European countries (Mascitelli and Chung, 2021) (CSR, 2020) (Lysne et al., 2019).

The United Kingdom aligns itself with US policy from the outset (Oughton & Frias, 2018). BT, the UK's leading telecommunications operator, has reached agreements with Ericsson and Nokia. For security reasons, the British government has demanded that its operators must not purchase equipment or technology from Huawei (Schaefer, 2020, p. 1502) (Ly and Ly, 2021, p. 95). The objective for 2027 is to operate 5G technology without Huawei's equipment. Italy has also prohibited the agreement between Fastweb and Huawei as its sole provider of the 5G core network (Rühlig & Björk, 2020, p. 25).

Germany has been particularly faced with the choice between its two major trading partners: the US and China.[33] Threats of economic or trade sanctions from one or the other have placed Germany's 5G policy in a serious and very worrying political-strategic context (Rühlig & Björk, 2020, p. 15). Precedents for similar international pressure are rarely identified.[34] While Telefonica and Nokia, for lack of other options, have stuck with Huawei, Deutsche Telekom and Vodafone have excluded the latter as a supplier.

France has adopted on August 1, 2019 the Law No 2019–810 (Rühlig & Björk, 2020, p. 25).[35] The title clearly shows its objective: "to preserve the interests of the defence and national security of France".[36] Colloquially known as the *anti*-Huawei law,[37] this regulation establishes a system of prior authorisation by the Prime Minister for the operation and functioning of such equipment and networks. The express purpose of this measure is to safeguard national defence and security interests. In February 2021, the Constitutional Council declared the constitutionality of this law for this reason (Constitutional Council, 2021).[38] But not all the problems that French law might raise are solved by this decision.

France is a member of the EU. This organization has been assigned extensive competences in matters that may be affected by national 5G legislation. And France, like all other member States, must act in compliance with EU competences and regulations. Despite having this national legal basis, which is legitimate and constitutional under French law, the requirement of prior authorisation regime included in the Law Nº 2019–810 could be in conflict with EU rules, in particular those concerning the liberalisation of the electronic communications and the internal market. In accordance with the well-established case law of the Court of Justice of the European Union, a system of prior national authorisation is rarely compatible with the liberalisation aim of the internal market.

The EU has acknowledged that the deployment and management of 5G networks is a matter of national security. But it has also recognised, precisely in the Commission's Communication "EU-China - A Strategic outlook", that the security of 5G networks is

[27] According to Article XXI, "Nothing in this Agreement shall be construed: a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests".

[28] On March 2021, US and China hold the first high-level meeting (https://www.china-briefing.com/news/us-china-relations-in-the-biden-era-a-timeline/?utm_source=DiploMail&utm_campaign=cb7e2a15e2-WeeklyDigest15_COPY_01&utm_medium=email&utm_term=0_4510155485-cb7e2a15e2-120324936).

[29] Jen Psaki, Press Secretary, stated that: "Telecommunications equipment made by untrusted vendors, including Huawei, is a threat to the security of the U.S. and our allies. We'll ensure that the American telecommunications network do not use equipment from untrusted vendors, and we'll work with allies to secure their telecommunications networks and make investments to expand the production of telecommunications equipment by trusted U.S. and allied companies" (https://www.whitehouse.gov/briefing-room/press-briefings/2021/01/27/press-briefing-by-press-secretary-jen-psaki-special-presidential-envoy-for-climate-john-kerry-and-national-climate-advisor-gina-mccarthy-january-27-2021/).

[30] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

[31] Alfayad considers the benefits for Gulf regions countries of the cooperation with Huawei and China in the context of US-China trade war (Alfayad, 2019). Canosa and Fiori explain the high commercial support of Huawei in Central American and Caribbean countries (Canosa and Fiori, 2019: 184). Quintana analyses the different reaction of Latin American countries to Huawei and 5G technology (Quintana, 2021).

[32] Actually, the Prague Proposals includes a direct reference to that issue: "The overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection" (https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/).

[33] According to the Prague Proposals, "Every country is free, in accordance with international law, to set its own national security and law enforcement requirements …" (https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/).

[34] To appreciate this situation, see the article Can International Law Survive a Rising China (Chesterman, 2020).

[35] The Fondation Concorde has published a report about French situation. The report highlights the impact of 5G technology over economy (Fondation Concorde, 2018).

[36] https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038864094.

[37] The evolution and nature of Huawei as a company can explain its leadership on 5G technology (Murmann, 2020) (Wen, 2017) (Fu et al., 2018). About its links with China, see Balding, 2019.

[38] https://www.conseil-constitutionnel.fr/decision/2021/2020882QPC.htm.

essential to ensure the strategic autonomy of the Union.[39] According to the Commission, "ensuring the cybersecurity and resilience of 5G networks is an issue of strategic importance for the Union"[40]. The Statement issued by the European Council, 2021 on March 25, 2021 stresses "the need to enhance Europe's digital sovereignty in a self-determined and open manner by building on its strengths and reducing its weaknesses and through smart and selective action, preserving open markets and global cooperation".[41] Although the concepts of digital autonomy and strategic sovereignty have not been defined in the EU framework, and although the real value of 5G may even be questioned by some authors, after these and other previous and subsequent statements, it seems clear that for the EU it is an essential value linked to the concept of digital sovereignty. In addition, the development of 5G technology affects several areas of EU competence, in particular the digital single market which is one of the essential pillars of the Union. And it is, in the European framework, a key component to ensure the EU's strategic autonomy and digital sovereignty.

5G is not only a key issue for Member States and the EU, but also an area where national and European competences come together in such a way that it is not always easy to determine the respective powers and the authority ultimately responsible. There are three additional problems. First, 5G affects several main areas of EU action and, in the absence of a common policy, there is a risk of fragmentation of the internal market and thus of the very foundations of European integration. Second, as the Commission pointed out, the interconnected and transnational nature of these infrastructures mean that any significant vulnerabilities and/or cybersecurity incidents concerning 5G networks happening in one Member State could have significant impacts beyond national borders.[42] Third, 5G the problem of technological dependence that can hardly be addressed by individual States acting alone. As Kaska pointed out, "a shared concern necessitates a coordinated response" (Kaska et al., 2019, p. 20).

There have also been some proposals focused on an EU/NATO coordination in this matter (Kaska et al., 2019, p. 20). However, considering the role of the US in this alliance, action in the NATO framework would not really be a European policy or even a response in line with European needs and interests. Moreover, by the nature of this organization, it would be a policy conceived in terms of security that would neglect the other dimensions of the 5G. Precisely, defending Europe's interest from commercial or anti-competitive practices, such as those emanating from China (Rühlig & Björk, 2020, p. 27), requires a joint European Union action.

As Rühlig and Björk argues, in the context of US and China competition, "Europe appears to have become not the only, but possibly the most important battleground. At first glance, it might appear that this puts Europe in a favourable position … however, Europe is actually in a rather weak position (…) given its enormous dependence on technology from both the US and China, Europe is technologically vulnerable" (Rühlig & Björk, 2020, p. 25). Politically, the EU has been somewhat displaced because European States are deploying their own 5G policies (CSR, 2020). And, in addition, legally, the EU can only act when it has been assigned the competences. Therefore, a main issue is to determine the competence and legal frameworks for EU action on 5G.

3. Competence and legal frameworks

The EU is an international organization that has only those competences attributed to it by the Member States, which are the original and principal holders of those competences. The EU has neither the ownership of competences nor general or unlimited powers. Instead, the EU is only allocated the capacity to exercise those powers that are conferred on it by the provisions of the Treaties. The European model of distribution of competences implies that the Union exercises competences in certain areas, while others remain within the Member States, and that the Union cannot exercise competences that have not been conferred on it in the European Treaties (Garben & Govaere, 2017) (Arena, 2016, p. 28). In addition, there are different categories of competences. The Treaty on the Functioning of the EU sets out the legal regime for competences in Articles 2 to 6. According to these rules, the EU has exclusive competences (Arts. 2.1 and 3), shared competences (Arts. 2.2 and 4), coordinating competences (Arts. 2.3 and 5), and supporting, promoting or complementary competences (Arts. 2.5 and 6). Differences between them are substantial.

Security in 5G networks is not defined as an EU competence in the Treaties. Nor is it a competence held entirely and exclusively by its Member States. Actually, 5G security materially and transversally concerns different areas in which the EU has competence and areas that fall within the competence of the States. But, in particular, it affects the main core of the EU's action, which is the internal market, in three main areas: 1) The legal regime for electronic communications (Kaska et al., 2019,p. 14); 2) The provisions on the security of networks and information systems; and 3) The latest regulations on cybersecurity. According to the Council and the Commission,[43] this corpus of rules is currently the main basis for EU action on 5G.

An analysis of the provisions of the Treaties and the acts adopted in application of them in this specific area shows that European policy on 5G network security is not the outcome of an autonomous policy, but is the result of the combination of these three regulatory pillars. However, each of these pillars poses its own set of problems.

The legal regime for electronic communications is currently embodied in Directive (EU) 2018/1972 establishing the European Code on Electronic Communications (ECEC), which was to be transposed by States by 21 December 20, 20.[44] According to the implementation report, particularly, the European Commission Recommendation 2019/534 on the cybersecurity of 5G networks, UE's action fits "into a broader European legal framework for the protection of electronic communications networks and their ecosystem,

[39] https://ec.europa.eu/info/sites/info/files/communication-eu-china-a-strategic-outlook.pdf.
[40] https://media.hotnews.ro/media_server1/document-2020-12-16-24488188-0-raport-impact-5g.pdf, p. 2.
[41] https://www.consilium.europa.eu/media/48976/250321-vtc-euco-statement-en.pdf.
[42] https://media.hotnews.ro/media_server1/document-2020-12-16-24488188-0-raport-impact-5g.pdf, p. 1.
[43] https://media.hotnews.ro/media_server1/document-2020-12-16-24488188-0-raport-impact-5g.pdf, p. 2.
[44] OJEU, L 321, 17.12.2018, pp. 36–214.

notably the European Electronic Communications Code which demands that all electronic communications service providers take appropriate security measures" .[45]

As the legal basis for EU policy on 5G, the ECEC regime raises two main issues.[46] The first is the use of the directive itself as a regulatory instrument. Unlike the EU regulation, it leaves a broad margin of action to the States. Most importantly, it implies that the rights and obligations for natural and legal persons, companies or users derive from the internal transposition rule - and not directly from the European one - which can lead to differences in terms of regulation between the different Member States. The second problem of the ECEC normative lies in the fact that, by March 2021, most of the Member States had not yet transposed this directive. Currently, the Commission has initiated infringement proceedings against many of them for non-compliance with their obligations by failing to transpose this European Code.[47] This situation creates considerable legal uncertainty at a key moment for 5G policy.

The legislation adopted under Directive (EU) 2016/1148 on measures to ensure a high common level of security of network and information systems across the Union,[48] known as the NIS Directive, establishes a legal regime that applies to operators of essential services and digital service providers. This directive focuses on security and incident reporting requirements. The application of this normative to 5G raises two issues too. The first is that the review process of the NIS Directive is already underway. This implies some regulatory uncertainty because the rules currently in force will not be the definitive ones in this area. The second problem is that Article 1.3 of the NIS Directive states that these provisions do not apply to companies subject to the electronic communications regime. Implementing the requirements of the NIS Directive to electronic communications in the context of 5G, when the Directive itself expressly excludes this possibility, is a serious legal problem. A possible solution would be to take advantage of the planned reform of the NIS Directive to change this provision and resolve the problem by requiring compliance with the same security requirements also in the field of electronic communications.

The Cybersecurity Act[49] has two distinct parts: the provisions concerning ENISA, which is designated as the EU Agency for Cybersecurity, and the regulation on the European Cybersecurity Certification Framework. Although significant progress has been made, there are two weak points in this second regulation: its progressive character and its voluntary nature, which do not allow a quick solution to be achieve in terms of the homogeneity of European certification.

In fact, within this regulatory triptych, the most solid legal framework is the ECEC Directive, which has not yet been transposed in many countries. The ECEC requires Member States to ensure that providers of public electronic communications networks or publicly available electronic communications services take appropriate and proportionate technical and organisational measures to adequately manage the risks to the security of their networks and services (Article 40). Although some of the measures are similar, they are not the same as those foreseen in the area of security of network and information systems. For instance, as an example, differences can be seen in relation to the parameters for determining the significance of a security incident in Article 40.2 of the ECEC Directive and Article 14.4 of the NIS Directive. Homogenising both regimes by maximising the level of security would be desirable, also with the aim of providing security requirements that are as uniform as possible in all areas. Finally, the implementation and enforcement of both regulatory regimes are similar, but stricter in the case of the ECEC.

As a whole, this European regulatory framework is insufficient and complex. In addition, these European regulations do not cover the typical regulatory elements identified as typical for 5G (Matinmikko et al, 2018). However, despite this, it has made it possible to build a European approach to 5G security.

4. The development of the European approach to 5G

Although there were some previous initiatives[50], the 5G Action Plan for Europe presented in 2016 by the Commission is the effective starting point for this European action (European Commission, 2016).[51] The main issue raised by this report on 5G is the risk of fragmentation in terms of spectrum availability, continuity of service across borders, as well as enforcement of rules, due to the uncoordinated national approaches existing up to that time.

The 5G Action Plan seeks appropriate coordination at European level on the basis of a number of measures: 1) A common timetable for 5G deployment; 2) The removal of obstacles to extend and facilitate 5G radio spectrum; 3) The multiplication of fixed and wireless connections; 4) The preservation of global interoperability; and 5) 5G innovation to support growth. As it expressly notes, the 5G Action Plan adopts an ambitious approach, but it is a document of the Commission, not of the institutions as a whole, and is not legally binding.

Already at that time, the possibility of acting with a more effective, legally binding standard at the European level seems complicated. On the one hand, the other main EU institutions have limited themselves to regulating specific aspects, as is the case with

[45] https://media.hotnews.ro/media_server1/document-2020-12-16-24488188-0-raport-impact-5g.pdf, p. 2.

[46] There are also other questions related to competition and other issues (Tsilikas, 2017), but there are material and not juridical or institutional challenges.

[47] On 4 February 2021, The Commission has opened infringement procedures against 24 Member States for failing to enact new EU telecom rules included in the European Electronic Communications Code (https://ec.europa.eu/commission/presscorner/detail/en/IP_21_206).

[48] OJEU, L 194, 19.07.2016, pp. 1–30.

[49] OJEU, L 151, 7.06.2019, pp. 15–69.

[50] Is the case of METIS that is an integrated project partly funded by the European Commission which started in November 2012. This project was designed with the objective of laying the foundation for 5G systems and building consensus prior to standardization (Osseiran et al., 2014, p. 26).

[51] https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-588-EN-F1-1.PDF.

the Decision (EU) of the European Parliament and of the Council of May 17, 2017 on the use of the 470–970 MHz frequency band. This decision expressly recognises that 5G networks will have a major impact not only on the digital sector, but on economies as a whole, and that the successful launch of 5G will be crucial for the economic development and for the competitiveness and productivity of the EU economies.[52] Despite this, there was clearly a lack of political will to introduce legally binding measures at the European level for 5G.

This conclusion was confirmed when EU Member States adopted the Tallinn Ministerial Declaration on 5G on 18 July 2017.[53] The use of a ministerial declaration – instead of an act of the Council-has important legal and political implications. The choice of this normative instrument is the legal evidence of the primary responsibility of States as well as of the consequent limitation of the EU's competences. The EU's role in 5G is therefore limited to the coordination of national actions and policies. Such a decision may be regrettable because, with some logic, a common European policy would be more competitive and more effective at the global level than individual national actions. Nevertheless, the coordination of national EU policies is a modality of EU competence with a long tradition and with appreciable results in areas such as economic, social and employment policies, that is regulated in Article 5 of the Treaty on the Functioning of the European Union.

In any case, the Tallinn Declaration deserves to be seen in a positive light insofar as it expresses a certain consensus among the Member States on 5G policy. Among some technical agreements, there are two main lines of actions: on the one hand, preserving global 5G interoperability through a comprehensive and inclusive approach as a priority for the Digital Single Market; and, on the other, establishing a strategic dialogue that could be extended to the whole multi-stakeholder community, including promoting early adopters and supporting peer-to-peer learning and transparency. The value of the function assigned to the EU emerges sometime later.

In March 2019, the European Council, 2019 asked the Commission for a proposal on a concerted approach to 5G network security,[54] which took the form of Recommendation (EU) 2019/534 of March 26, 2019 on the Cybersecurity of 5G networks (Dominioni & Rugge, 2020, , p. 9) (European Commission, 2019).[55] The main contributions of this Recommendation are threefold. The first is that it strengthens European competence in this area by recognising that 5G is a priority within the Digital Single Market Strategy because it is the backbone of a wide range of services essential for the functioning of the internal market and the maintenance of vital social and economic functions. A second particularly noteworthy contribution of this Recommendation is that it provides a comprehensive and global definition of 5G networks as "the set of all network infrastructure elements relevant to mobile and wireless communications technologies used in connectivity and value-added services with high performance characteristics, such as very high data rates and capacities, low latency communications, ultra-high reliability or support for a high number of connected devices". The third contribution of this Commission act is the establishment of the objectives, measures and procedures for organising the security of 5G. To this end, the first step focuses on action at national level through a risk assessment of 5G infrastructure developed by Member States. The second phase has to be performed at the EU level with two main actions: a coordinated risk assessment and the adoption of a common set of tools to address the risks.

This Commission Recommendation is explicitly endorsed by the Council of the EU in December 2019 in its Conclusions on the importance of 5G technology for the European economy and the need to mitigate 5G-related security risks (Council of the European Union, 2019).[56] In addition, the Council introduces two main principles in this regard. On the one hand, it recognises that the fast and secure introduction of 5G networks is essential to improve EU competitiveness and requires a coordinated EU approach, without prejudice to Member States' competences. On the other hand, it makes a fundamental point by stating that "building trust in 5G technologies is firmly rooted in the EU's core values -such as human rights and fundamental freedoms, the rule of law and the protection of privacy, personal data and intellectual property-in the commitment to transparency, reliability and inclusiveness of all stakeholders and all citizens". Placing 5G policy in the context of the EU's foundations, values and principles has a significance that goes beyond the merely symbolic as it defines the nature and legitimacy of its action in this area.

5. Procedures and instruments

Following the support of the Council, and thus of the Member States, the operational programme set out in Recommendation 2019/534 has been launched. In July 2019, the national assessments are sent to the Commission and ENISA to provide, together with ENISA's technical report, the basis for a coordinated EU risk assessment (EURAC5G), which is adopted on October 9, 2019 (Section 5.1). This assessment is, in turn, the basis for the development of the EU Toolbox on 5G Cybersecurity (EUT5G) that is adopted on January 29, 2020 (Section 5.2).

5.1. The EU coordinated risk assessment of the cybersecurity of 5G networks (EURAC5G)

EURAC5G is defined as a high-level report agreed by the Member States, with the support of the Commission and ENISA, setting out the main common conclusions resulting from national risk assessments on 5G networks (NIS Cooperation Group, 2019).[57] It is not an

[52] OJEU, L 138, 25.05.2017, pp. 131–138.
[53] https://mmpi.gov.hr/UserDocsImages/arhiva/Ministerial-declaration-5G-final-signed.pdf.
[54] https://www.consilium.europa.eu/en/press/press-releases/2019/03/22/european-council-conclusions-22-march-2019/.
[55] OJEU, L 88, 29.03.2019, pp. 42–47.
[56] https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.
[57] https://www.politico.eu/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf.

exhaustive study, but it is rather focused on elements of strategic importance for the EU. It is, in its terms, the first step in a process aimed at ensuring the long-term and sustainable security of 5G networks. Although it is not a legal text, EURAC5G reflects a basic consensus that may lead the way to a higher level of commitment.

EURAC5G assumes the definition of 5G networks made in Recommendation 2019/534, identifying three of its technical characteristics that constitute a substantial difference from the previous situation, namely: 1) The move towards software and virtualisation through technologies such as Software Defined Network (SDN) and Network Functions Virtualisation (NFV); 2) The development of Network Slicing; and 3) Greater functionality at the edge of the network and a less centralised architecture. After defining the general framework, the EURAC5G follows the risk assessment methodology of ISO/IEC 27005, 2018 [58] This evaluation covers the following elements: threats, actors, assets, vulnerabilities, risks and related scenarios.

The main *threats* are those related to confidentiality, availability and integrity. These include local or global disruption of 5G networks, espionage, modification or rerouting of traffic or data, or destruction or disruption of other infrastructure or systems over 5G networks. *Actors* are classified into various categories: accidental/non-adversarial, individual hackers (erroneously defined as amateur criminals or lobbyists), action groups, insiders, State agents and other possible actors from corporations to cyber-terrorists. *Assets* are evaluated by categorising logical and functional components including the core and access functions defined in the 3GPP (3rd Generation Partnership Project) and the underlying functions, not defined in the 3GPP, of transport and transmission, network exchange and management systems and support services. *Vulnerabilities* are classified into several categories distinguishing between those related to hardware, software, processes and policies and those related to suppliers. *Risk scenarios* are identified by distinguishing between the following: 1) those arising from insufficient security measures, such as network misconfiguration or lack of access controls; 2) those related to the 5G supply chain, such as equipment failures or vulnerabilities or reliance on a single vendor; 3) those arising from the modus operandi of threat actors; 4) those resulting from the interdependency between 5G networks and other critical systems; and 5) those caused by users' devices.

EURAC5G explicitly recognises that 5G technology creates a new security paradigm that requires a re-evaluation of the current regulatory framework. In order to respond to the challenges raised in EURAC5G, the EU Toolbox on 5G Cybersecurity is adopted on January 29, 2020.

5.2. The EU toolbox on 5G cybersecurity (EUT5G)

The EUT5G is based on a main principle: the security of 5G networks is essential to protect economies and societies and to ensure the technological sovereignty of the Union (NIS Cooperation Group, 2020).[59] The main objective of EUT5G is to define a coordinated European approach based on 5G security and compatible with the internal market.

The EUT5G is a system set out in a document agreed within the Cooperation Group created in the framework of the NIS Directive in which Member States, the Commission and the European Cybersecurity Agency are represented. By its nature, it is not a legally binding text. As expressly recognised, it only expresses the solid commitment of the States and the Commission to use and implement the recommended measures following the envisaged methodology to address the risks identified in the EURAC5G (Dominioni & Rugge, 2020, p. 10).

Following the model of allocation of competences included in the EUT5G, Member States have the following responsibilities: 1) Strengthening security requirements for mobile network operators; 2) Assessing the risk profile of suppliers; and 3) Establishing a supplier strategy aimed at ensuring an appropriate balance of suppliers at national level, avoiding or limiting reliance on a single or any high-risk provider, and ensuring that each operator has a multi-supplier strategy. The Commission, together with the States, has two main roles to play: 1) Facilitate coordination between them on standardization and certification; and 2) Promote a diverse and sustainable 5G supply chain to avoid long-term dependency by building on existing instruments and strengthening the EU's 5G capabilities with programmes and funding.

The EUT5G sets out three types of measures: strategic, technical and supporting actions. Risk mitigation plans should consist of possible combinations of these types of measures depending on the nature and extent of the risk, which may be classified as very high, high, medium or low. The measures will be adopted by national or European authorities.

In September 2020, the report on the implementation by States of the EUT5G is published and the Commission adopts Recommendation C (2020), 6270 final, on a common EU toolkit to reduce the cost of deploying very high capacity networks and to ensure timely and investment-friendly access to 5G radio spectrum, in order to foster connectivity in support of the economic recovery from the COVID-19 crisis (European Commission, 2020a)[60]. In October, the European Council, 2020 called on the EU and the Member States "to make full use of the 5G cybersecurity Toolbox adopted on January 29, 2020, and in particular to apply the relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments, based on common objective criteria".[61] The European Council states that potential 5G suppliers need to be assessed on the basis of common objective criteria.

[58] https://www.iso27001security.com/html/27005.html.
[59] https://www.politico.eu/wp-content/uploads/2020/01/POLITICO-Cybersecurity-of-5G-networks-EU-Toolbox-January-29-2020.pdf.
[60] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020H1307&from=EN.
[61] https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf, p. 5.

6. Implementation and further development

There are two main inputs concerning the current situation and the perspectives of evolution of EU action on 5G: the evaluation made by the Commission in December 2020 (Section 6.1) and the new European Cybersecurity Strategy (Section 6.2) that was also adopted in December.

6.1. The evaluation of the commission

The Report on the impacts of the Commission Recommendation of March 26, 2019 on the Cybersecurity of 5G networks was published on 16 December 20, 20 (European Commission, 2020b).[62] According to this report, Member States were highly appreciative of the overall process for several reasons. First, they found it an unprecedented method of cooperation leading to the definition of an ambitious and coordinated EU framework for 5G cybersecurity while preserving flexibility in view of the national security aspects. Secondly, they qualified Europe's coordinated action on 5G as timely, effective and proportionate. Thirdly, they agreed on the collaborative approach between national authorities, the Commission, ENISA and other relevant stakeholders that was considered suitable to address this complex issue that cuts across EU and Member State competences.

The definition of common objectives and methodologies at the European level is consistent with the adoption of national measures by Member States adapted to their national circumstances. In addition, at the operational level, the process to develop the EU Coordinated risk assessment and the Toolbox was considered well-structured. National authorities worked together within a dedicated Work Stream of the NIS Cooperation Group, with the support of the Commission and ENISA. Finally, from a politico-strategic perspective, the report recognised that there is a need to continue to pay attention to international developments and to consolidate a common EU voice and vision towards third country partners.

In this period, Member States, with the support of the Commission, ENISA and BEREC, had worked to develop a Toolbox of mitigating measures. There are both strategic and technical measures.[63]

There are three main developments at the level of strategic measures. First, a large majority of Member States have adopted or are at a final stage of adopting the legal framework to strengthen the regulatory powers of national authorities to be able to impose strengthened obligations on operators and to impose restrictions or prohibitions. Second, measures aimed at applying restrictions based on the risk profile of suppliers have been adopted, proposed or planned in nearly all Member States and only a small minority of countries have yet to define clear plans to implement these measures. Third, several Member States have introduced measures concerning suppliers' diversification and resilience. Many of them are asking for further exchanges on this issue at EU-level and for exploring possible practical guidance for national approaches.[64]

The situation is somewhat different concerning technical measures. Although a majority of Member States has made good progress in implementing the technical measures of the Toolbox, there are States that have not done so and many of them have not even transposed the ECEC Directive. Besides, some Member States are adding specific requirements for 5G or are planning to introduce new measures while others consider their current measures as sufficient or have no plans for changes. That is not the best scenario for progress at the European level. Nevertheless, most of the supporting action included in this European Commission's report was also included in the EU's Cybersecurity Strategy that was adopted the same day, which reflects an increased commitment of the Member States.

In addition, on September 18, 2020, the Commission has adopted the Recommendation 2020/1307 on a common Union toolbox for reducing the cost of deploying very high-capacity networks and ensuring timely and investment-friendly access to 5G radio spectrum, to foster connectivity in support of economic recovery from the COVID-19 crisis in the Union.[65] Following this recommendation, at the end of March 2121, EU Member States have agreed on a Union-wide Connectivity Toolbox[66] "aims at fostering connectivity across the EU by (i) reducing the cost and increasing the speed of deploying VHCN and (ii) ensuring a timely and investment-friendly access to 5G radio spectrum". To this end, Member States have to work together and in close cooperation with the Commission. A Special Group, the Connectivity Special Group, has been created in order to identify and share best practices and assist Member States, upon request, in the implementation of the Toolbox.

[62] https://media.hotnews.ro/media_server1/document-2020-12-16-24488188-0-raport-impact-5g.pdf.

[63] Following the report, "Strategic measures (SM) cover measures concerning increased regulatory powers for authorities to scrutinize network procurement and deployment, specific measures to address risks related to non-technical vulnerabilities, as well as possible initiatives to promote a sustainable and diverse 5G supply and value chain in order to avoid systemic and long-term dependency risks. Technical measures (TM) include actions to strengthen the security of 5G networks and equipment by addressing the risks arising from technologies, processes, human and physical factors" (https://media.hotnews.ro/media_server1/document-2020-12-16-24488188-0-raport-impact-5g.pdf, p. 6).

[64] According to Rühlig and Björk, "Diversification of supply chains combines two dimensions. First, Europe should import technology and raw materials from as many different suppliers from as many different countries as possible. Second, Europe should avoid dependency on technology that relies on patents from one country in order to avoid being dragged into the patent wars that loom behind Trump's entity list. This strategy of diversification should be combined with the use of all available means under WTO law to preserve free trade and fair competition" (Rühlig & Björk, 2020, p. 27).

[65] OJEU, L 305, 21.09.2020, p. 33.

[66] https://www.mtitc.government.bg/sites/default/files/theconnectivitytoolboxpdf.pdf.

6.2. The European Cybersecurity Strategy

The EU's Cybersecurity Strategy for the Digital Decade, adopted in December 2020, included several references to 5G. However, the two main contributions are, on the one hand, the proposal to export the European Toolbox model to third countries and, on the other hand, the appendix dedicated to determining the next steps for 5G. According to the Strategy, the EU's 5G Toolbox approach has raised interest in non-EU countries. For that reason, "the Commission services together with the European External Action Service and the network of EU delegations, stands ready to provide additional information if requested on its comprehensive, objective and risk-based approach to authorities around the world" (European Commission, 2020c).[67] Alongside this, the only Appendix to the Strategy text is dedicated to 5G. It includes priorities, objectives and measures to achieve them, as well as the identification of those responsible in each case: States, the Commission, ENISA, relevant authorities and other stakeholders.

There are three *priorities*. The first is to complete the implementation of the 5G Toolbox at national level, to address the issues identified in the progress reports and to enhance coordination work or exchange of information with the aim of promoting development of best practices or guidance. The second priority is the continuous monitoring of evolutions in the technology, 5G architecture, threats and 5G use cases and applications, as well as external factors, in order to be able to identify and address new or emerging risks. The third one is to continue EU-level actions both to support and complement the Toolbox objectives and to fully integrate them into relevant EU policies. The areas concerned by 5G are growing and more EU competences have been involved in its regulation.

There are also three key *objectives*. For each of them, areas, mainly short- and medium-term actions and responsible actors are identified.

A) The first key objective is to ensure convergent national approaches for effective risk mitigation across the EU. To this purpose, there are three areas of work and three main actions: a) Complete the implementation of the measures recommended in the Toolbox which is a task for the Member States authorities; b) Intensify exchanges of information and consider possible best practices on strategic measures related to suppliers concerning, in particular, restrictions on high-risk suppliers, measures related to the provision of managed services as well as supply chain security and resilience. In this case, the lead actors are Member States authorities and the Commission; and c) Develop capacity building and guidance on technical measures which is a responsibility assigned to ENISA and Member States authorities.
B) The second key objective is supporting continuous exchange of knowledge and capacity building through four areas of work: a) Continuous knowledge building on technology and related challenges; b) Risk assessments through the update and exchange of national information; c) Joint EU-funded projects to support the Toolbox implementation with the necessary financial support; and d) Cooperation among stakeholders. The Member States authorities, the Commission and ENISA are the lead actors for these different tasks, except for the Joint EU projects in which ENISA is excluded.
C) The third key objective is to promote supply chain resilience, and other EU strategic security objectives in five areas: a) Standardization[68]; b) Supply chain resilience[69]; c) Certification[70]; d) EU capacities and secure network[71]; e) External aspects. At this regard, the action envisaged is to respond favorably to third country requests who would like to understand and potentially use the Toolbox approach developed by the EU. This task is assigned to Member States, the Commission and EU Delegations (European Commission, 2021).[72]

Finally, on March 2021, the Council has adopted the Conclusions on the EU's Cybersecurity Strategy for the Digital Decade. It stresses the importance of a coordinated approach as well as the development and implementation of effective measures at national level to reinforce the security of 5G networks. The Council supports the review of the Commission's Recommendation in order to define a long-term and comprehensive approach looking at the entire 5G value chain and ecosystem (Council of the European Union, 2021).[73] According to the document, the Council "highlights, while emphasizing Member States' responsibility for the protection of national security, its strong commitment to applying and swiftly completing the implementation of the EU 5G Toolbox measures and to continuing efforts made to guarantee the security of 5G networks and the development of future network generations. The close cooperation between Member States, the Commission and ENISA on security of 5G networks could serve as an example for other issues

[67] https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade, p. 10.
[68] The main action is to define and implement a concrete action plan to enhance EU representation in standard setting bodies. The lead actors are the Member States but, perhaps, it would have been useful to involve the Commission in this task since this institution has the competence to represent the EU.
[69] It is a responsibility for the Member States and the Commission that has to be fulfilled through two main measures: analyze of the 5G ecosystem and supply chain to identify and monitor key assets and critical dependencies; and ensure the functioning of 5G market and supply chain according to the EU trade and competition rules. Member States authorities and the Commission are the lead actors in this task.
[70] The intended action is to initiate preparations of relevant candidate certification schemes for key 5G components and suppliers' processes with the leadership of the Commission, ENISA, the national authorities and other stakeholders.
[71] Two actions are planned: investment into research, innovation and capacities; and implement relevant security conditions. Lead actors are Member States, the Commission, the 5G industry and stakeholders.
[72] The question of Europe's digital leadership and global competitiveness on 5G has been included among the objectives of 2030 Digital Compass (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118).
[73] https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf.

in the field of cybersecurity while respecting the competences of the Member States and the principles of subsidiarity and proportionality".

7. Conclusions

5G technology has been defined as a key component for the development of the economy and society as a whole. 5G has also become a source of international controversy. Whether directly or indirectly through their technology companies, the US and China are at the centre of a controversy in which the defence of national interests and security is intertwined with the struggle for hegemony in the technological, political and strategic domains.

The EU recognises the existence of a national security issue for Member States and also the strategic value of 5G for the Union as a whole. But it has neither the means nor the competences to enter into such competition with the world leaders in 5G technology. EU Member States lack the technological base and lack all the necessary powers to manage 5G independently because some of the competences needed have been conferred to the EU or may affect EU competences. Moreover, no individual State can have the same capacity and potential to respond to this problem and to the pressures of third States as would a coordinated action of all the countries in the framework of the EU.

Since the adoption of the 5G Action Plan in 2016, and on the basis of the competences attributed to the EU in the areas of electronic communications, network and system security, cybersecurity and certification, a European 5G policy has been progressively built up so far. The analysis of this process, its nature and characteristics, the subjects involved and the measures adopted to achieve its objectives allows some conclusions to be reach in relation to the three main questions addressed in this research.

The objective of achieving technological autonomy and digital sovereignty has become a priority within the EU and has been consistently reiterated by the Member States and the EU institutions. This objective is attached to the EU and not to its Member States individually, the fact that it is a common, European, rather than a national or individual objective, is of enormous significance. It is recognition of the commitment to European action, despite the fact that it is a matter of State competence. Whereas States are still appealing to their sovereign status in the physical world in the traditional sense, the idea of digital sovereignty is associated with EU activity.

Having decided on the preference for joint European action, it is necessary to define the model for the organization of the European and national competences. According to Article 2 of the Treaty on the Functioning of the European Union, the EU can exercise different types of competences, ranging from exclusive or shared competences, to coordinating competences or supporting, promoting and complementary competences. Among these options, the coordination of national policies is the method chosen for 5G. A model of exclusive or shared competences would not necessarily be a better option considering that for many Member States this is a matter of security and national interest. Moreover, national policy coordination has proven to be an effective and operational, as well as realistic, method in other areas of particular relevance such as economic, social or employment policies.

Therefore, the EU has the competence to coordinate Member States' national 5G policies. In other words, the EU cannot legislate or adopt legally binding acts in the area of 5G, as this is the responsibility of the Member States. However, the Member States are bound by the coordination model established at European level for the definition, implementation and evaluation of the measures adopted in this field. For now, the main coordination procedures and instruments have been the EURAC5G and the EUT5G as well as the implement evaluation developed by the Commission.

The European 5G model can be explained clearly and transparently by distinguishing between the regulatory legal responsibilities of States and the coordinating legal responsibilities of the EU. Rules and acts with legal effects for third parties are the responsibility of the individual Member States. The objectives, subjects, measures, procedures and instruments are the result of European coordination, mainly through soft law norms, which includes both the programming phase and the evaluation of results.

The technological dependency imposed by 5G technology is a fact which can only be addressed with some guarantee of effectiveness through action at European level. No Member State has the capacity to overcome this situation, neither would it be feasible within the digital single market itself, which does not allow for any autonomous national policies. This situation can only be addressed with a European policy which, due to its size and components, could constitute an alternative to the pre-eminence of other States and companies coming from or being supplied by other countries.

In the short term, such a European policy should be built through EU coordination of national policies and following a strategy of supplier diversification which, in itself, would increase competition and reduce the perverse effects of technological dependence. In the medium and long term, the objective should be more ambitious. Following the multi-stakeholder model, a consortium of European companies, with strong European funding or even public participation, justified by the public good or service nature of 5G, could be a solution to external dependency. The support of economic actors for a European policy was already made public in December 2019 in a Declaration by the CEOs of major telecommunications operators and service providers on the purpose of digital networks.[74] A European policy based on the coordination of national policies of the Member States and a multi-stakeholder governance model are, for the time being, the way towards strategic autonomy and European digital sovereignty.

[74] https://etno.eu/news/all-news/655-ceos-statement-digital-networks.html.

Acknowledgements

Work partially supported by Spanish Government through Project PID 2020-114495RB-I00 and by Network Engineering & Security Group (NESG). Funding for Open Access Charge: Universidad de Granada / CBUA

References

5G Americas. (2020). *The 5G evolution: 3GPP releases* (pp. 1–54). 5G.
Agiwald, M., Roy, A., & Saxena, N. (2016). *Next generation 5G wireless networks. A Comprehensive Survey. IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617-1655*. IEEE.
Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A. S., & Ylianttila, M. (2019). Security for 5G and beyond. *IEEE Communications Surveys & Tutorials, 21*(4), 3682–3722.
Alfayad, F.S. (2029). Huawei and the Gulf region: Market opportunities despite the ongoing US-China trade war. International Review of Management and Marketing, vol. 9 (4), pp. 47-53.
Akyildiz, I. F., Nie, S., Lin, S.-C., & Chandrasekaran, M (2016). 5G roadmap: 10 key enabling technologies. *Computer Networks, 106*, 17–48.
Alon, I., Zhang, W., & Lattemann, C. (2021). *The case for regulating Huawei* (pp. 1–3). FIIB Business Review.
Andrews, J. G., et al. (2014). What will 5G Be? *IEEE Journal on Selected Areas in Communications, 32*(6), 1065–1082.
Arena, A. (2016). Exercise of EU competences and pre-emption of member states' powers in the internal and the external sphere: Towards 'grand unification? *Yearbook of European Law, 35*(1), 28–105.
Balding, C. (2019). *Huawei technologies' links to Chinese state security services*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726.
Boccardi, F., et al. (2014). Five disruptive technology directions for 5G. *IEEE Communications Magazine, 52*(2), 74–80.
Brake, D. (2018). *Economic competitiveness and national security dynamics in the race for 5G between the United States and China*. HIS Economics & HIS Technology.
Cai, Y., et al. (2018). Modulation and multiple access for 5G networks. *IEEE Communications Surveys & Tutorials, 20*(1), 629–646.
Campbell, K., et al. (2017). *The 5G economy; How 5G technology will contribute to the global economy*. HIS Economics & HIS Technology.
Canosa, N., & Fiore, G. (2019). China vs. Estados Unidos: Huawei y el núcleo de la disputa. *Revista de Derecho, Política y Sociedad* (pp. 179–187). Bordes.
Cartwright, M. (2020). Internationalizing state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review, 9*(3), 1–18.
Cave, M. (2018). How disruptive is 5G? *Telecommunications Policy, 42*(8), 653–658.
CRS-Congressional Research Service. (2020). *TikTok: Technology overview and issues*. Available at:https://fas.org/sgp/crs/misc/R46543.pdf https://crsreports.congress.govR46543.
Constitutional Council. (2021). *Décision n° 2020-882 QPC du 5 février 2021*. Available at: https://www.conseil-constitutionnel.fr/decision/2021/2020882QPC.htm.
Council of the European Union. (2019). *Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G, 14517/19, Brussels, 3.12*. Available at: https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.
Council of the European Union. (2021). Conclusions on the EU's cybersecurity strategy for the digital decade. Available at: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf.
Chesterman, S. (2020). Can international law survive a rising China?. *NUS law working paper 2020/018*. National University of Singapore.
Dominioni, S., & Rugge, F. (2020). *The geopolitics of 5G*. ISPI Dossier.
Drahokoupil, J., McCaleb, A., Pawlicki, P., & Szunomár, Á. (2017). Huawei in Europe: Strategic integration of local capabilities in a global production network. *Chinese investment in Europe*. Brussels: European Trade Union Institute (ETUI).
ENISA. (2019). *Threat landscape for 5G networks*. Available at: https://www.enisa.europa.eu/news/enisa-news/enisa-draws-threat-landscape-of-5g-networks.
Erie, M. S., & Streinz, T. (2021). *The beijing effect: China's "digital silk road" as transnational data governance*. New York University Journal of International Law and Politics.
European Commission. (2016). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "5g for Europe: An action plan"* (p. 588). Brussels: COM.
European Commission. (2019). *Joint Communication to the European Parliament.* the European Council and the Council, "EU-China – A strategic outlook".
European Commission. (2020a). *Recommendation on a common Union toolbox for reducing the cost of deploying very high capacity networks and ensuring timely and investment-friendly access to 5G radio spectrum, to foster connectivity in support of economic recovery from the COVID-19 crisis in the Union*.
European Commission. (2020b). *Report on the impacts of the commission recommendation of 26 March 2019 on the cybersecurity of 5G networks, commission staff working document.* SWD.
European Commission. (2020c). *Joint communication to the European parliament and the Council "the EU's cybersecurity strategy for the digital decade"*. Available at: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.
European Commission. (2021). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "2030 digital Compass: The European way for the digital decade". Available at:. *Use capitals letters: "Parliament", "Economic" "Social" "Committee", "Regions" "Digital"* (p. 118) COM https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.
European Council. (2019). *Conclusions, 22 March 2019*. Available at: https://www.consilium.europa.eu/en/press/press-releases/2019/03/22/european-council-conclusions-22-march-2019/.
European Council. (2020). *Special meeting of the European Council (1 and 2 october 2020)*. Available at: Conclusions https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf.
European Council. (2021). *Statement of the members of the European Council on 25 March 2021*. Available at: https://www.consilium.europa.eu/media/48976/250321-vtc-euco-statement-en.pdf.
Fondation Concorde, F. (2017). *La 5G: Prendre le virage du monde d'après* (pp. 1–65). FC.
Fu, X., Sunb, Z., & Ghauric, P. N. (2018). Reverse knowledge acquisition in emerging market MNEs: The experiences T of Huawei and ZTE. *Journal of Business Research, 93*, 202–215.
Garben, S., & Govaere, I. (2017). *The division of competences between the EU and the member states*. London: Hart Publishing.
Gil, P., et al. (2017). *Despliegue automático de aplicaciones NFV y SDN para detectar y mitigar ciberamenazas en redes 5G. Actas de las III Jornadas Nacionales de Investigación en Ciberseguridad*. Madrid: Universidad Rey Juan Carlos.
Gupta, A., & Jha, R. K. (2015). A survey of 5G network: Architecture and emerging technologies. *IEEE Access, 3*, 1206–1232.
Houser, K. A. (2020). The innovation winter is coming: How the U.S.-China trade war endangers the world. *San Diego Law Review, 57*, 549–608.
Hussain, S. R., Echeverria, M., Karim, I., Chowdhury, O., & Bertino, E. (2019). 5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol. Available at:. *In 2019 ACM SIGSAC conference on computer and communications security (CCS '19)* New York: ACM. https://doi.org/10.1145/3319535.3354263.
ITU. (2020). 5G - Fifth generation of mobile technologies. Available at: https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx.
I, C., Rowell, C., Han, S., Xu, Z., Li, G., & Pan, Z. (2014). Toward green and soft: A 5G perspective. *IEEE Communications Magazine, 52*(2), 66–73.
ICANN. (2020). *5G technology*. ICANN Office of the Chief Technology Officer.
Inkster, N. (2019). The Huawei affair and China's technology ambitions. *Survival, 61–1*, 105–111.
ISO/IEC 27005. (2018). *Information technology — security techniques — information security risk management*. Available at: (3rd ed.) https://www.iso27001security.com/html/27005.html.

Janusch, H., & Lorberg, D. (2020). *Maximum Pressure, Minimum Deal: President Trump's Trade War with a Rising China. S&F Sicherheit und Frieden*. nomos-elibrary.de. Available at: https://www.researchgate.net/profile/Holger-Janusch-2/publication/346155850_Maximum_Pressure_Minimum_Deal_President_Trump%27s_Trade_War_with_a_Rising_China/links/5ff33df5299bf140886fe630/Maximum-Pressure-Minimum-Deal-President-Trumps-Trade-War-with-a-Rising-China.pdf.

Kaska, K., Beckvard, H., & Minárick, T. (2019). *Huawei, 5G and China as a security threat*. Tallin: NATO Cooperative Cyber Defence Centre of Excellence.

Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2020). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials, 22*(1), 196–248.

Li, Y., & Li, T. (2021). Construction of enterprise 5G business ecosystem: Case study of Huawei. *American Journal of Industrial and Business Management, 11*, 92–110.

Lysne, O., et al. (2019). *Critical communication infrastructures and Huawei. TPRC47: The 47th research Conference on communication*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3426222.

Mackenzie, M. (2010). Securitizing sex. *International Feminist Journal of Politics, 12*(2), 202–221.

Matinmikko, M., et al. (2018). On regulations for 5G: Micro licensing for locally operated networks. *Telecommunications Policy, 42*(8), 622–635. https://doi.org/10.1016/j.telpol.2017.09.004

Mascitelli, B., & Chung, M. (2021). Huawei, China, and ideological tensions in the 5G telecommunications platforms. *Global Challenges and Strategic Disruptors in Asian Businesses and Economies, IGI Global*, 141–152.

Medina Serrano, J. C., Papakyriakopoulos, O., & Hegelich, S. (2020). Dancing to the partisan beat: A first analysis of political communication on TikTok. Available at:. In *12th ACM Conference on web science* https://www.semanticscholar.org/paper/Dancing-to-the-Partisan-Beat%3A-A-First-Analysis-of-Serrano-Papakyriakopoulos/9a58d301a32acb9e83ae152dd8263c4f0ce0a894.

Meese, J., Frith, J., & Wilken, R. (2020). *COVID-19, 5G conspiracies and infrastructural futures* (Vol. 177, pp. 30–46). Media International Australia.

Declaration, Ministerial (2017). *Making 5G a success for Europe*. Available at: https://mmpi.gov.hr/UserDocsImages/arhiva/Ministerial-declaration-5G-final-signed.pdf.

Ministry of Energy, Tourism and Digital Agenda. (2018). *Spain's 5G national plan 2018-2020*. https://avancedigital.mineco.gob.es/5G/Documents/plan_nacional_5G_en.pdf.

Murmann, J. P. (2020). *The management transformation of Huawei: An overview*. Available at:https://www.researchgate.net/publication/340098400_The_Management_Transformation_of_Huawei_From_Humble_Beginnings_to_Global_Leadership. Cambridge University Press.

Navarro-Ortiz, J., Romero-Diaz, P., Sendra, S., Ameigeiras, P., Ramos-Muñoz, J. J., & Lopez-Soler, J. M. (2020). A survey on 5G usage scenarios and traffic models. *IEEE Communications Surveys & Tutorials, 22*(2), 905–929.

NIS Cooperation Group. (2019). *EU coordinated risk assessment of the cybersecurity of 5G networks*. Available at: https://www.politico.eu/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf.

NIS Cooperation Group. (2020). *Cibersecurity of 5G networks EU toolbox of risk mitigating measures*. Available at: https://www.politico.eu/wp-content/uploads/2020/01/POLITICO-Cybersecurity-of-5G-networks-EU-Toolbox-January-29-2020.pdf.

Noble, M., Mutimear, J., & Vary, R. (2019). *Determining which companies are leading the 5G race, Wireless technology*. Wireless Technology.

Osseiran, A., et al. (2014). Scenarios for 5G mobile and wireless communications: The vision of the METIS project. *IEEE Communications Magazine, 52*(5), 26–35.

Oughton, E. J., & Frias, Z. (2018). The cost, coverage and rollout implications of 5G infrastructure in Britain. *Telecommunications Policy, 42*, 636–652.

Prague 5G Security Conference. (2019). Available at:. *Prague Proposals* https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

Quintana, A. R. (2021). *Latin American countries must not allow Huawei to develop their 5G networks. Issue brief No. 6041* (pp. 1–8). Douglas And Sarah Allison Center for Foreign Policy.

Rao, S. K., & Prasad, R. (2018). Impact of 5G technologies on industry 4.0. *Wireless Personal Communications, 100*, 145–159.

Rost, P., et al. (2016). Mobile network architecture evolution toward 5G. *IEEE Communications Magazine, 54*(5), 84–89.

Rühlig, T., & Björk, M. (2020). *What to make of the Huawei debate? 5G network security and technology dependency in Europe*. Swedish Institute of International Affairs.

Schaefer, K. J. (2020). Catching up by hiring: The case of Huawei. *Journal of International Business Studies, 51*, 1500–1515.

Shoebridge, M. (2018). *Chinese cyber espionage and the national security risks Huawei poses to 5G networks*. Available at: Macdonald-Laurier Institute Publication https://www.macdonaldlaurier.ca/files/pdf/MLICommentary_Nov2018_Shoebridge_Fweb.pdf.

Stritzel, H. (2014). Securitization theory and the copenhagen School. *Security in translation. New security challenges series*. London: Palgrave Macmillan.

Tsilikas, H. (2017). Huawei v. ZTE in context – EU competition policy and collaborative standardization in wireless telecommunications. *IIC, 48*, 151–178.

US. (2019). *National defence authorization act*. Available at: https://www.congress.gov/115/crpt/hrpt676/CRPT-115hrpt676.pdf.

US. (2020). *The national strategy to secure 5G*. available at: https://www.ntia.doc.gov/files/ntia/publications/booz_allen_hamilton-06252020.pdf.

US. (2021a). *National strategy to secure 5G implementation plan*. Available at: https://www.ntia.gov/files/ntia/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final.pdf.

US. (2021b). *President executive order on America's supply chains*. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

Wen, Y. (2017). *The rise of Chinese transnational ICT corporations: The case of Huawei*. Available at: Simon Fraser University https://summit.sfu.ca/item/17505.

West, D. M. (2016). *Achieving sustainability in a 5G world* (pp. 1–16). Washington DC: Center for Technology Innovation at Brookings.

Yan, X., & Huang, M. (2020). *Leveraging university research within the context of open innovation: The case of Huawei*. Telecommunications Policy.