JONES DAY | One Firm Worldwide®

WHITE PAPER

May 2020

Member State Implementation of the EU 5G Toolbox: Legal Issues Raised

In January 2020, the European Commission endorsed the Toolbox of mitigating measures agreed by the Member States of the European Union to address security risks related to the rollout of 5G. The protection of national security, and cybersecurity in particular, are unquestionably legitimate objectives. However, since protecting these interests may contravene ordinarily applicable laws and principles, EU and international law provide for exceptions to enable the adoption of such security-related measures. These are not open-ended instruments, though, and must be applied subject to essential safeguards.

Certain Toolbox measures could raise legal risks, depending on their actual implementation by Member States. The present *White Paper* focuses on three Strategic measures ("SM") presented in the Toolbox, as their implementation could raise a number of legal concerns. Specifically, these SM relate to: (i) expanding the role of national authorities (SM01), which may lead to additional and questionable authorization regimes; (ii) screening for high-risk suppliers and imposing restrictions on the use of equipment from such suppliers (SM03), potentially resulting in the outright and unwarranted exclusion of certain suppliers; and (iii) multi-vendor strategies (SM05), which cannot be interpreted as a market share cap that would unjustifiably reduce the number of suppliers on the market.

TABLE OF CONTENTS

I. EU 5G TOOLBOX

In January 2020, the European Commission ("Commission") endorsed the Toolbox of mitigating measures agreed by the Member States of the European Union to address security risks related to the rollout of 5G ("Toolbox").[1] The Toolbox responds to 5G network security concerns in the European Union, notably arising due to alleged ties between certain telecom equipment suppliers and foreign governments, and China in particular. In seeking to protect national security, and particularly with regard to cybersecurity, these are unquestionably legitimate EU objectives, and Member States are competent to protect such objectives.

The Toolbox has received broad support from the industry and market participants and is generally regarded as a positive step. The Toolbox sets out a series of recommended measures aimed at ensuring 5G network security (i.e., 18 measures (eight Strategic measures and 11 Technical measures) and 10 supporting actions).

The Toolbox's measures, which are generally sensible and risk mitigating, can positively impact 5G security. Depending on their actual implementation in the Member States, nonetheless, certain Toolbox measures could raise legal risks. It is important to recall that the European Union is (inevitably) an environment where Member States' national interests sometimes lead to resisting the EU rule of law. Thus, implementation of the Toolbox should not become a further example of Member States' shortcomings in adhering to the EU legal order.

Among the Strategic measures in the Toolbox, three raise particular concerns regarding Member State implementation and the proper respect of EU legal principles:[2]

- Strategic Measure 1 (SM01): "Strengthening the role of national authorities";
- Strategic Measure 3 (SM03): "Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk—including necessary exclusions to effectively mitigate risks—for key assets"; and
- Strategic Measure 5 (SM05): "Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies".

These three measures are potentially particularly intrusive and also raise concerns in terms of their implementation. Sections, II, III and IV below outline certain key legal issues and principles under EU and international law that Member States should recall in implementing the Toolbox, and particularly in relation to the above three Strategic measures.

Importantly, various exceptions to EU and international law exist in view of safeguarding the imperative need for national security and cybersecurity. Under certain conditions, therefore, measures otherwise inconsistent with ordinary legal obligations can be justified in the interest of protecting specific objectives. As discussed below in Section , however, such measures are subject to stringent conditions, particularly as concerns proportionality. Thus, critical substantive and procedural constraints must be kept in mind by Member States, where seeking to rely on such exceptions in implementing measures in furtherance of the Toolbox.

II. SM01: STRENGTHENING THE ROLE OF NATIONAL AUTHORITIES

Under SM01, Member States can take measures in view of "strengthening the role of national authorities". In this respect, the Toolbox refers to the "regulatory powers for national authorities" and the possibility to, *inter alia*, "use ex-ante powers to restrict, prohibit and/or impose specific requirements or conditions, following a risk-based approach, for the supply, deployment and operation of the 5G network equipment".[3]

Towards implementing SM01, some Member States have introduced (or are considering doing so) an authorization regime whereby mobile network operators ("MNOs") must obtain national government approval before deploying their network, in view of allowing authorities to screen the equipment used. At the outset, it is questionable whether such type of authorization regime falls under measures contemplated under SM01. In any event, to the extent that Member States establish an authorization regime for the provision of electronic communication networks under SM01, they should take into account the legal considerations below.

First, procedurally, it is questionable whether such an authorization regime can be entrusted to any other authority than the national regulatory authorities ("NRAs"), or other competent authorities associated with regulating electronic communications over the years. The Toolbox, which is based on Article 13a of the Framework Directive,[4] explicitly refers to "regulatory powers for national authorities", as well as their "ex ante powers"

to impose certain conditions.[5] The EU regulatory framework thereby already provides for the regulatory powers of NRAs.

Assigning competence for such authorization regime (or similar powers) to a Member State body other than NRAs would jeopardize protections under Article 6 of the European Electronic Communications Code ("EECC"),[6] whereby competent authorities must present guarantees of independence and impartiality.[7] Such non-NRA oversight would also potentially deprive MNOs of other important rights and protection, including: the right to appeal all decisions to a court or another body independent of external intervention or political pressure,[8] the protection of confidential commercial information (related to deployment plans) guaranteed by the regulatory framework,[9] and extensive case law framing the exercise of such regulatory powers over the past 30 years.

Second, such specific authorization system under SM01 (and eventually the enabling of equipment screening prior to network deployment) is at odds with the regulatory framework that established a general authorization system which ensures the freedom to provide electronic communications networks and services, without any restriction (except for the possibility to request a notification).[10] Member States may not require an operator "to obtain an explicit decision or any other administrative act by such authority or by any other authority before exercising the rights derived from the general authorization".[11] It is therefore legally uncertain whether conditions pertaining to the security and integrity of 5G networks can be imposed on top of conditions attached to general authorizations and subsequent to the award of spectrum. At a very minimum, any such restriction must be properly reasoned and notified to the Commission.[12]

Third, while conditions may be attached to general authorizations, these are exhaustively listed in Annex I to the EECC. Annex I B (5) of the EECC provides that one such possible condition is the security of public networks against unauthorized access, for the purpose of protecting the confidentiality of communications and the maintenance of network integrity. These conditions may be modified, but only under the terms of Article 18 of the EECC, which require objective justifications, proportionality, and prior notice and consultation. Furthermore, where authorization relates to radio equipment and technology used by an MNO for exercising its rights of use for spectrum, it may also be viewed as restricting *ex post* such rights of use, which is also subject to conditions and can require adequate compensation.[13]

Fourth, an authorization system under SM01 could amount to the re-establishment of exclusive and special rights, which are contrary to Article 106(1) TFEU combined with Article 102 TFEU[14] and to secondary EU legislation. This would occur if the criteria underpinning such authorization were not objective, proportional and non-discriminatory. In this regard, the Terminal Equipment Directive[15] clearly states that "it is necessary to abolish all existing exclusive rights in the importation, marketing, connection, bringing into service and maintenance of terminal and telecommunications equipment, as well as those rights having comparable effects—that is to say, all special rights except those consisting in legal or regulatory advantages conferred on one or more undertakings and affecting only the ability of other undertakings to engage in any of the abovementioned activities in the same geographical area under substantially equivalent conditions".[16]

Additionally, to the extent that such authorization would be limited in time, this could disincentivize MNOs from relying on equipment from specific suppliers. If MNOs lack sufficient certainty as to their ability to procure equipment from certain suppliers in the long term, this will deter them from buying from those suppliers, also potentially triggering interoperability issues and related costs. As such, an authorization regime under SM01 that is limited in time may act as a *de facto* ban, triggering implementation concerns similar to those in relation to SM03 below.

III. SM03: RESTRICTIONS ON EQUIPMENT FROM "HIGH-RISK" VENDORS

SM03 provides for screening of suppliers to identify high-risk vendors ("HRV") and the possible imposition of restrictions on the use of equipment from an HRV for key assets. The Toolbox explains that "one of the key aspects in the assessment" when screening for HRVs relates to the "likelihood of the supplier being subject to interference from a non-EU country". In this context, various elements would be relevant, such as the cybersecurity policy of the third country having jurisdiction over the supplier, "a strong link between the supplier and a government of a given third country" and "the ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment".[17] The HRV screening therefore risks being intrinsically linked to the country of origin of the equipment supplier and to targeting

non-EU equipment suppliers specifically. The Toolbox also affirms the goal of ensuring the European Union's technological sovereignty.[18]

At least indirectly, the HRV screening raises the risk of effectively favoring "home-grown" companies and targeting non EU-based suppliers that may be the most technologically advanced. In some Member States,[19] stakeholders are even suggesting that HRV screening should focus *only* on the country of origin of the supplier, irrespective of any technical or other considerations.

Depending on a Member State's implementation, the HRV screening mechanism can therefore lead to potentially barring certain non-EU vendors because of the origin of the supplier and its products. This would raise concerns, irrespective of whether such bar would be explicit or a *de facto* consequence of the mechanism and irrespective of whether the bar is total or applies only to specific parts of the network. HRV screening further raises the possibility of a very broad interpretation that would encompass the recall of 4G equipment already in use. This, in turn, would trigger legal issues and technical obstacles to 5G deployment.

A far-reaching interpretation of HRV screening would infringe various core EU law principles. First, it would restrict the free movement of goods and services (Articles 34 TFEU and 56 TFEU) insofar as such HRV measure would in fact target the sale of equipment (manufactured in the European Union or already in free circulation in the European Union) and provision of services.

Certain fundamental rights would also be violated, such as the: (i) right to property (Article 17 of the Charter[20]), in that it could lead to prohibiting the use of certain non-EU suppliers' 5G equipment and even the eventual recall of their 4G equipment already in use (since 5G networks would need to re-use such equipment); and (ii) freedom to conduct a business (Article 16 of the Charter) by limiting non-EU suppliers in their economic activity in the European Union, and by restricting MNOs in their ability to contract with a desired equipment supplier.

The HRV screening mechanism also raises potential concerns under various non-discrimination standards. Specifically, under EU law, such screening may infringe the principle of technological neutrality, as the ban on non-EU equipment (and *de facto* the use of Chinese equipment) would effectively favor specific technology solutions originating from EU-based equipment manufacturers. Moreover, if HRV screening is not grounded upon objective technical standards or past evidence of security breaches, but rather on vague and subjective criteria based on the supplier's country of origin, this would violate the principle of non-discrimination and equal treatment (Article 18 TFEU and Articles 20 and 21 of the Charter).

EU Member States must also recall their international obligations. Specifically, a ban that is *de facto* based on the supplier's country of origin would violate the Most-Favored-Nation principle and National Treatment principle (Article III:4 of the GATT), which are key principles under World Trade Organization ("WTO") law (Article I:1 and Article III:4 of the GATT) and Bilateral Investment Treaties ("BITs").

IV. SM05: MULTI-VENDOR STRATEGY

Under SM05, the Toolbox recommends "ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies", and in particular, ensuring that "each MNO has an appropriate multi-vendor strategy to avoid or limit any major dependency on a single supplier (or suppliers with a similar risk profile), ensure an adequate balance of suppliers at national level and avoid dependency on suppliers considered to be high risk".[21]

The promotion of supplier diversity, in principle, is pro-competitive. However, legally speaking, the multi-supplier measure cannot be interpreted in a way that it would effectively establish a pre-defined market share cap on certain equipment suppliers, and thus artificially limit such suppliers' activities in the European Union. This could lead to excluding more efficient and technically superior providers, in violation of EU law. This legal risk would be exacerbated, if basing implementation of a market share cap on the supplier's country of origin.

To a large extent, the issues identified in relation to a wide-ranging interpretation of HRV screening, as discussed above, would apply *mutatis mutandis*. Concerns regarding special rights are particularly relevant to a multi-sourcing strategy. By limiting competition from certain suppliers, and in particular non-EU vendors, European-based operators would enjoy a form of regulatory protection akin to special rights. This

violates primary and secondary EU legislation. Indeed, Article 106 (1) TFEU (combined with another Treaty provision such as Article 102 TFEU, the free movement or non-discrimination rules) and the Terminal Equipment Directive prohibit the granting of special and exclusive rights, i.e., regulatory measures that confer on one or a limited number of undertakings legal or regulatory advantages that are not based on objective, proportional and non-discriminatory criteria.

In addition, Member States should be aware that implementing a multi-vendor strategy can raise additional legal concerns. Specifically, setting an eventual maximum cap on the proportion of equipment that a single manufacturer can provide within a network would clearly depart from a key principle driving economic policy since the early days of the European Communities (later the European Union), i.e., undistorted competition to ensure equality between efficient operators. Indeed, settled case law states that operators must be allowed to compete on the merits. Thus, in pursuing the legitimate goal of ensuring sufficient diversification of supply, Member State implementation of a multi-vendor strategy must legally ensure access to the most efficient supplier and equality of opportunity among all equipment suppliers. Effectively, all suppliers must be treated on an equal footing.

V. NATIONAL SECURITY EXCEPTIONS AND THE PRINCIPLE OF PROPORTIONALITY

As the above-discussed panoply of fundamental, long-standing rules may restrict a country's ability to pursue legitimate objectives such as the protection of national security, EU and international law provide for a number of exceptions. Such exceptions, however, are not open-ended and are subject to essential safeguards.

The EU electronic communications regulatory regime foresees the possibility for Member States, on the grounds of national security, to restrict the freedom to provide electronic communications networks and services. However, this does not afford Member States with an unlimited ability to respond to cybersecurity concerns. The public security derogation applies narrowly as an exception to EU law. This derogation is subject to the mandatory provisions of the regulatory framework, as well as to general principles of EU law, including the principles of proportionality and non-discrimination.

Among the mandatory provisions of the regulatory framework, the safeguard clause of the Radio Equipment Directive[22] is particularly relevant. This Directive harmonizes standards on radio equipment and contains a safeguard clause in Articles 40 and 42. Under these provisions, national authorities must comply with substantive and procedural requirements when taking corrective measures for safety or other public interest reasons. These include a notification to the Commission and other Member States. The safeguard clause must also be interpreted strictly.

As ruled by the European Court of Justice ("ECJ"), protective measures adopted under the safeguard clause cannot be based on a purely hypothetical risk, nor founded on mere suppositions that are not yet scientifically verified.[23] To the extent that network equipment is considered as radio equipment within the meaning of the Radio Equipment Directive (as is the case for passive equipment, specifically RAN-equipment), a Member State seeking to adopt restrictive measures against such equipment (for public interest reasons) would be required to respect the safeguard procedure and thus first inform the Commission.

Measures adopted in derogation of EU law, in view of safeguarding national security and public policy, must be proportionate to the goal pursued. In this respect, the ECJ found a national rule subjecting the sale of radio equipment to a national-type approval scheme (*Radiosistemi*) to be disproportionate.[24] The principle of proportionality entails a three-prong test that requires measures that: (i) are appropriate to attain the objectives pursued (i.e., "suitability test"); (ii) do not go beyond what is necessary to achieve these objectives (i.e., "necessity test"); and (iii) strike a fair balance between the different interests at stake (i.e., "proportionality test '*stricto sensu*'" or absence of excessive effect).

Depending on the approach to implementation, the above-identified Strategic measures in the Toolbox raise risks under each of these three tests:

The Suitability Test: Measures that target suppliers from a specific country are in disregard of the global nature of information and communications technology ("ICT") supply chains. They also fail to acknowledge the critical role of MNOs, who are best placed to grasp complex supply chains and ensure network safety. A comparative assessment of equipment of suppliers impacted by measures, with equipment of

suppliers not impacted, would also be highly relevant. Any measure that fails to objectively assess all suppliers could thus raise concerns.

The Necessity Test: An existing comprehensive regime already regulates electronic communications services, including 5G. Such regime allows Member States, NRAs and in practice MNOs (as the ultimate party bearing cybersecurity obligations) to ensure the integrity of their telecom networks. Any imposition of additional obligations must gauge the effectiveness of existing rules and procedures.

The Proportionality Test *Stricto Sensu*: As the Strategic measures described above can have far-reaching consequences for the supplier concerned (ultimately leading to exclusion from the market), these must be regarded as the most intrusive forms of regulatory intervention. Accordingly, their application must be carefully considered within both the existing regulatory framework, as well as other possible regulatory intervention (e.g., enhanced interoperability requirements; additional conditions on certification of equipment; strengthening investigation powers of national authorities over equipment suppliers; adopting a code of good conduct; imposing reporting obligations, etc.) The Strategic measures also raise the risk of less efficient 5G networks, and any assessment of their proportionality must also integrate the long-term negative impacts of these measures on competition and consumer welfare. In general, the proportionality test *stricto sensu* would require a fact-based approach. For instance, a *de facto* ban is unlikely to meet this standard in the absence of any actual evidence of wrongdoing.

Furthermore, implementation of the Strategic measures must be even-handed and in line with the non-discrimination principle, which is raised into doubt, given the focus on the country of origin. Finally, Member States must actually demonstrate that the alleged risk to national security and public policy is real, not abstract or hypothetical.

Similar comments apply to the public morals/policy exception provided for by WTO law. Not all of the above conditions are present under the national security exception under WTO law, but such WTO exception applies only in specifically defined circumstances, such as "in time of war or other emergency in international relations", which is arguably unfulfilled here. While certain BITs contain extensive public security exceptions, there are equally BITs that do not include such exceptions or limit the possibility to invoke these to specific violations.

VI. CONCLUSION

Following the adoption of the Toolbox, Member States are requested to develop national measures to ensure 5G cybersecurity and report on these measures by the end of June 2020. The Toolbox is a set of guidelines, or "possible approaches" that could be taken by Member States to mitigate a previously identified security risk and after reviewing the effectiveness of existing measures. The above analysis reveals that SM01 (if used to provide for an authorization regime), SM03 and SM05 are particularly prone to raising a number of legal concerns. These are, however, only three out of the 18 measures and 10 supporting actions foreseen by the Toolbox. In other words, the Toolbox offers a range of mitigating measures to choose from, and not all of these measures necessarily present the same legal risks.

In any event, irrespective of the combination of measures chosen, any implementation at Member State level has to keep in mind the legal boundaries of a potential national regulation, as set out above. Specifically, key principles such as promotion of competition and equal treatment and non-discrimination have to be complied with. Taking into account the global nature of the ICT supply chain and the principle of non-discrimination, any measure must apply to all equipment suppliers and not only those from third countries.

The proportionality principle will also be particularly relevant to assess the legality of any national measure. In this context, it will be important for any implementing measure to be based on actual evidence of cybersecurity threats, taking into account all relevant facts and circumstances. The proportionality of any national measures must also be assessed against alternative less-restrictive measures (e.g., enhanced interoperability requirements, additional conditions for the certification of equipment, strengthening the investigation powers of NRAs vis-à-vis equipment suppliers or adopting a code of good conduct), even if these are not explicitly foreseen in the Toolbox.

LAWYER CONTACTS

Yvan N. Desmedt
Amsterdam / Brussels
+31.20.305.4203 / +32.2.645.15.23
ydesmedt@jonesday.com

Laurent De Muyter
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

Eva Monard
Brussels
+32.2.645.15.10
emonard@jonesday.com

Alexandre G. Verheyden
Brussels
+32.2.645.15.09
averheyden@jonesday.com

Laurence N. Van Mullem, an associate in the Brussels Office, assisted in the preparation of this White Paper.

ENDNOTES

1 Cybersecurity of 5G networks—EU Toolbox of Risk-Mitigating Measures, 29 January 2020.

2 EU Toolbox, page 12.

3 EU Toolbox, page 20.

4 Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services ("Framework Directive").

5 EU Toolbox, page 20.

6 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

7 NRAs must adhere to substantive guarantees when imposing *ex ante* regulatory obligations. They must act impartially, objectively, transparently and in a non-discriminatory and proportionate manner (see Article 3 (4) of the EECC).

8 See Article 31 and recital 46 EECC.

9 Article 20 (3) EECC.

10 Article 12 EECC.

11 Article 12 (3) EECC.

12 See Article 12 (1) EECC.

13 Article 19 EECC.

14 Treaty on the Functioning of the European Union ("TFEU").

15 Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment ("Terminal Equipment Directive").

16 See Recital 3 of the Terminal Equipment Directive.

17 EU Toolbox, p. 42 (including footnote 48). *See also* page 21, which refers to the risk factors identified in paragraph 2.37 of the EU Coordinated Risk Assessment.

18 Cybersecurity of 5G networks—EU Toolbox of Risk-Mitigating Measures, 29 January 2020, p. 3.

19 For instance, the Belgian security services stated the following in a hearing of the Belgian Parliament (at page 12): "As regards the risk analysis, the Belgian security services base themselves conceptually on the geostrategic risk profile of 5G equipment suppliers and not on technical elements. This geostrategic approach implies that, irrespective of a specific supplier or of the quality of that supplier's product, the services will take account of the risks that can result from a number of characteristics of the country from where that supplier originates".

20 Charter of Fundamental Rights of the European Union ("Charter").

21 *See* Q&A on the EU Toolbox.

22 Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment ("Radio Equipment Directive").

23 Case C-236/01, *Monsanto*, 9 September 2003, paras 106 and 107.

24 Joined cases C-388/00 and C-429/00, *Radiosistemi*, 20 June 2002 para. 45.