# European Commission 5G Recommendation

## Toolbox - Suggested Risk Factors and Management Tools

### 1. The 5G Recommendation and Suggested Member State Action

The European Commission's Recommendation of 26 March 2019 for cybersecurity in 5G networks (the "**5G Recommendation**"), instructs Member States to take a concerted approach to 5G security. By 30 June 2019, Member States shall **carry out a risk assessment of the 5G networks**. Member States are therefore instructed to create and agree on a so-called toolbox by 31 December 2019, which shall include:

- An inventory of security risks for 5G networks, covering two different risk categories; (i) technical factors and (ii) "other" factors; and,

- A set of proposed mitigating measures to address the risks.

**This report focuses on the risk category "other" factors and suggests specific criteria against which such risks should be assessed (section 2 below)**. Thus, in short, it is a basic indicative model for assessing risks associated with "other" factors.

This report also highlights legal aspects relevant for Member States to effectively enforce risk mitigating measures (section 3 below).

### 2. Basic criteria for assessing "other" risk factors

### 2.1 Importance of distinguishing between "other" (introduced) and technical factors

The 5G Recommendation makes a clear distinction between technical factors and "*other*" factors. A similar distinction is often made in the information and communication technology ("**ICT**") sector, where technical risks can be compared to a product's "inherent vulnerabilities". These include defect quality or unintentional deficiencies in ICT software, service or hardware. Addressing such risks is generally not controversial, as the supplier's and buyer's interests are aligned, such interests being to supply/buy functioning and secure hardware or software.

The category "other" factors covers external factors, and also includes so-called "introduced vulnerabilities", which refers to an intentional or unintentional manipulation of the supplier's hardware, software or service. In ICT security, *introduced*

*vulnerabilities*, are usually deemed to stem from illegitimate and covert motives by a third party.[1]

The 5G Recommendation lists a number of aspects to consider in the "other" factors category:

> "…inter alia, the overall risk of influence by a third country, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions…whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection."[2]

The following subsections list factors that could be included in a risk inventory of "other" factors.

## 2.2 Non-transparency

A 5G security risk assessment will necessarily require information and cooperation from the suppliers of 5G services, software and equipment (the "**Suppliers**") concerning both technical and "other" factors. As 5G security relates to national security, the burden of proof to substantiate any claim or assertion should fall on the Supplier. If a Supplier fails to be transparent or to cooperate when asked to provide information, such failure should in itself be considered a risk factor.[3]

Transparency requirements should cover, for example:

---

[1] See NCSC paper A Framework for Assessing Risk: https://www.dni.gov/files/NCSC/documents/products/SCRM_Framework_for_Assessing_Risk_White_Paper.pdf; see also page 4 to 7 of Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, U.S. House of Representatives, 112th Congress, October 8, 2012. Available at: https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf. See also section 8 of the Analysis of vulnerability to espionage, by the General Intelligence and Security Service of the Netherlands (AIVD), Directorate General for Safety and Security (DGV) Ministry of BZK: https://fas.org/irp/world/netherlands/aivd-vuln.pdf.

[2] The 5G Recommendation, page 4.

[3] Compare export control requirements for end-user information, see The Wassenaar Arrangement Participating States' non-exhaustive List of Advisory Questions for Industry, https://www.wassenaar.org/app/uploads/2018/12/Advisory-Questions-for-Industry-Amended.pdf. Compare also to the proposed French rules in *code des postes et des communications électroniques* where the operators are responsible for the application for authorisation, http://www.assemblee-nationale.fr/15/propositions/pion1722.asp.

1. Disclosure of information on ownership, control and financing of the Supplier and/or tiers of Suppliers, and in particular, if such ownership, control or financing is connected to a foreign state.[4]

2. Intelligence sharing agreements between Suppliers and tiers of Suppliers.[5]

3. Providing information on any legal requirements for Supplier and tier Suppliers to disclose information to foreign states.

### 2.3 Dependencies to foreign states – risk of influence

A primary focus in an inventory of "other" factors should be the discovery of any links or degree of dependency between a particular supplier and a foreign state. Such dependencies may affect the Supplier's autonomy and decision-making. Dependencies might also influence or encourage the Supplier to take operational or business decisions in relation to 5G network customers, which are not based primarily on the Supplier's own strategic and economic rationale, but are driven by a foreign state's foreign or security policy.

The dependency factor can be broken down into four subcategories:

1. **A state's direct or indirect ownership**: If a Supplier is owned by a foreign state, that state will de facto control the Supplier leading to clear risk of foreign state influence. However, partial and indirect state **ownership should also be considered.** Such assessments should be aligned with any reviews under the EU's new framework for foreign direct investment ("**FDI**") screening.[6]

---

[4] See Supply Chain Vulnerabilities from China in the U.S. Federal Information and Communication Technology, https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-20180516-SD105-U105.pdf, page 13, which states that "[F]*inancial links to suspect entities, including state-owned or substantially state-controlled enterprises, are also important for SCRM [Supply Chain Risk Management], as they indicate potential vectors for nefarious influence*."

[5] *Id.* page 16, which analyses corporate intelligence-sharing agreements: "*Commercial partnerships that share program application data, configuration information, or even deployment policies, however may inadvertently grant malicious actors information they need to infiltrate federal ICT systems*".

[6] See article 4.2 a and recital 13 of the new Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (the "**EU's FDI screening framework**"). Italy had already adopted a law for the screening of foreign investments in the fields of defense and national security as well as energy, transportation and communications (Italian Law Decree no. 21/2012). Such piece of legislation has entrusted the Government with extraordinary powers, enabling it to impose specific requirements and to veto corporate transactions in the sectors in question. Such powers can be also enforced in respect of

2. **Control**: Even if a foreign state does not hold direct or indirect ownership, it may have the ability to control a Supplier through governance structures or through the legal framework of the jurisdiction where the Supplier has its seat. The EU's Best Practice in relation to sanctions could provide suitable guidance for determining the level of control.[7]

3. **Financial influence**: A Supplier that receives state funding or state-backed funding may face exposure to influence by that state. This factor is also specifically mentioned in the EU's FDI screening framework as an important factor to consider.[8]

4. **Political influence**: A Supplier may have other ties to a foreign state, for example, if the Supplier is subject to legal or formal requirements of political representation in its administrative board, management board or council.[9] An example could be if a Supplier has voluntarily changed its articles of association to consult political committees before important decisions are made.[10]

---

contracts for the supply of goods and services regarding the design, manufacturing, maintenance and management of broadband electronic communication networks with 5G technology, to be provided by non-EU individual or entities. It is prescribed that any purchase of high technological content components, which may be functional to the above mentioned design or management activities, are subject to prior notice (it must be noticed that this is a recent amendment: see, Article 1*bis* of the draft bill of the Conversion Law of Legislative Decree n. 22, 2019, concerning the so-called Hard Brexit, which has been approved by the Senate on 23 April 2019 and is currently under approval by the lower house of Parliament – Camera dei Deputati). Link:
https://www.normattiva.it/urires/N2Ls?urn:nir:stato:decreto.legge:2012-03-15;21!vig= and
http://www.camera.it/temiap/documentazione/temi/pdf/1155963.pdf?_1556191521255.

[7] See Best Practice available on the website of the European Council:
https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf.

[8] See, footnote 6, and, for instance, an account of state influence over the financial sector in China, points 2.5 – 2.8 of the WTO document China's Trade-Disruptive Economic Model, Communication from the United States, WT/GC/W/745, of 16 July 2018.

[9] *Id.* section B. See also Global Times Published: 2016/12/18 21:53:39
http://www.globaltimes.cn/content/1024360.shtml.

[10] According to the following articles, a large number of listed Chinese companies have reportedly changed their articles of association to ensure that party committees are consulted prior to important decisions:
https://asia.nikkei.com/Politics/Chinese-enterprises-write-Communist-Party-s-role-into-charters,
https://asia.nikkei.com/Politics/Chinese-corporate-sector-falls-further-under-party-s-sway, see also reports from EU and the German Chambers of Commerce raising concerns that foreign-owned JVs in China are being encouraged to formalize party organisations within the JVs, giving the party a governance and decision-making role in matters significant to the JV:
http://www.europeanchamber.com.cn/en/press-releases/2583/chamber_stance_on_the_governance_of_joint_ventures_and_the_role_of_party_organisations,

## 2.4 Conflicting laws of foreign states

The 5G Recommendation explicitly lists foreign governance models, which naturally includes legal regimes, that a Supplier is subject to. Thus, the jurisdiction of a Supplier's headquarters or parent company is highly relevant, as the Supplier's parent company is by law subject to such legal regimes. Furthermore, any subsidiaries of the parent company, e.g. a Supplier established in the EU, could also be required to comply with such laws, either by the wording of the law (*de lege*) or through a *de facto* extraterritorial application of those laws. There is a consequential risk that, if a parent company is required to comply with certain laws, it will instruct its foreign subsidiaries to align with such legal requirements.[11]

It is critical to examine whether provisions of such foreign legal regimes are or could come in conflict with fundamental EU or national Member State laws or security interests.

The following provides three relevant examples of when a 5G Supplier could be faced with a situation where the laws in the EU conflict with foreign laws.

1. Under EU law, confidentiality of communication (including the communication of companies), is a fundamental right.[12] Restrictions on this right are only allowed in very limited and narrowly defined circumstances.

2. The EU's rules on data privacy as set out in the General Data Protection Regulation ("GDPR").

3. Legal regimes that could apply in relation to a state's national intelligence gathering. For example, the Chinese National Intelligence Law (the "NIL") [13] sets out broad

http://china.ahk.de/news/single-view/artikel/press-statement-increasing-business-challenges-delegations-of-german-industry-commerce-in-china-concerned-about-growing-influence-of-chinese-co/?no_cache=1.

[11] By comparison, US and EU sanctions are often directly or indirectly (by way of company policy) extended to subsidiaries outside of the US or the EU.

[12] See C-450/06 Varec SA, ECLI:EU:C:2008:91. See also the Charter of Fundamental Rights of the European Union and Directive 2002/58/EC.

[13] A risk factor imbedded in the construction of a law like NIL is the possible extraterritorial application. There are no explicit geographical limits of NIL. Thus, organisations could potentially refer to an entire group, including both parent company and overseas subsidiaries. Further, because NIL covers Chinese citizens, there is also an effective control over a European subsidiary if the management consists of Chinese citizens (those citizens will likely have a separate legal obligation to comply with NIL). A parent company could also simply decide to replace management or key functions in an EU company with Chinese citizens to effectively obtain such *de facto* extraterritorial application. See also, a general introduction of the Draft National Intelligence law in China, June 2018, available at:

obligations on Chinese organisations and citizens to cooperate, when requested, with Chinese authorities in regards to intelligence gathering. These obligations could have a *de facto* extraterritorial reach to subsidiaries, e.g. European subsidiaries, of Chinese parent companies.[14]

### 2.5 Legal regime in a Supplier's home jurisdiction: rule of law and separation of powers in the foreign legal regime

When assessing the laws of foreign states, and their effect on Suppliers, it is equally important to consider the foreign state's general governance model over its citizens and companies. In particular, a review should focus on the status of the judicial system, the respect for the rule of law and whether there is adequate separation of powers.

The rule of law is a fundamental principle enshrined in Article 2 of the Treaty of the European Union.[15] It includes legality, which implies a transparent, accountable, democratic and pluralistic process for enacting laws; legal certainty; prohibition of arbitrariness of the executive powers; independent and impartial courts; effective judicial review including respect for fundamental rights; and equality before the law.[16] It is important to distinguish and understand the difference between the *rule of law* and *rule by law*. For example, China has introduced the concept of *rule by law*, to legalize and institutionalize the party's leadership. However, the Chinese leadership does not appear to intend to copy "Western 'constitutionalism,' 'separation of powers,' or 'judicial independence.'"[17]

The assessment of a foreign state's governance model is therefore essential in order to assess whether a Supplier of 5G services, software or hardware in the EU, which may be affected by foreign law, has effective means of preventing and legally opposing a request from e.g. a foreign intelligence authority (in the parent company's jurisdiction)

---

https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html

[14] See English translation of the Chinese National Intelligence law, in particular article 7, available at: http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law

[15] Article 2 reads: "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail."

[16] See explanations provided in the European Parliaments Briefing from 2016, "Understanding the EU Rule of Law" available at http://www.europarl.europa.eu/EPRS/EPRS-Briefing-573922-Understanding-EU-rule-of-law-mechanisms-FINAL.pdf

[17] See article from Diplomat, citing an article by the Chinese President; available at https://thediplomat.com/2019/02/xi-china-must-never-adopt-constitutionalism-separation-of-powers-or-judicial-independence/. See also further explanations and sources set out on: https://sinopsis.cz/en/lawfare-by-proxy-huawei-touts-independent-legal-advice-by-a-ccp-member/.

to assist in interception that is illegal in the EU or contrary to an EU Member State's security.

Many countries have intelligence laws through which authorities may ask for cooperation from operators to assist in foreign intelligence gathering. However, in countries with a strong tradition of the rule of law and separation of powers, the scope of the law will normally be clearly defined and award a strong protection for fundamental rights. Decisions to ask operators to assist will consequently more likely be taken by an independent and often judicial authority, which has powers separate from the government or ruling party.

For the purpose of evaluating whether a foreign state affords private entities judicial protection to challenge state influence, the combination of the following parameters may be assessed:

1. Whether the domestic directives or laws have a clear and narrowly defined purpose, such as national security threats (e.g. terrorism), and which thus cannot be relied on to require operators to conduct interception of communication in general;

2. If the legal system has an independent judicial control function, i.e. that decisions to intercept communication are made by independent judicial authorities (e.g. judge); and,

3. The legal system is built on a clear separation of powers which ensures the independence of judges in relation to governing parties or governmental authorities requesting the decision.

Two examples of how these components work together are found in cases from the US and Canada.[18]

[18] The US case (*United States v. Microsoft Corp*.) from 2017 concerned whether Microsoft was obliged to provide the US authorities with data stored in Ireland according to a warrant. The court of appeals ruled in favour of Microsoft and invalidated the warrant. Link to United States v. Microsoft Corp: https://www.bloomberg.com/news/articles/2019-02-24/huawei-frightens-europe-s-data-protectors-america-does-too, and https://www.reuters.com/article/us-microsoft-usa-warrant/microsoft-wins-landmark-appeal-over-seizure-of-foreign-emails-idUSKCN0ZU1RJ. The character of the Canadian case is similar to the US case. A Federal Court judge ruled, in July 2018, that the scope of Canadian intelligence is strictly limited to the domestic territory, unless national security is at stake. Accordingly, the independent judge effectively hindered a widening of the scope of the law, such judgement made possible through the approval procedure and the separation of powers. Link to the Canadian case: https://www.theglobeandmail.com/canada/article-judge-limits-canadas-international-spying-reach/.

## 3. Risk management measures/methods

The 5G Recommendation instructs Member States to draw up appropriate, effective and proportionate "risk management measures" to mitigate the identified cybersecurity risks at national and Union level.[19] This section addresses a number of legal issues that the Member States should address, in order to ensure that any risk management measures have a legal basis and are enforceable.

### 3.1 Legal basis for Member States to take measures

A pre-requisite for applying relevant risk management measures is that Member States have a legal basis to implement such measures.

As a first step, Member States should ensure that they have implemented the two directives specifically listed in the Recommendation[20] to secure that their national authorities may (i) impose security requirements on network operators, and if necessary, issue binding instructions to them, and (ii) when granting general authorisations for electronic communication, attach conditions to protect the security of the network against unauthorised access.[21]

### 3.2 Effective enforcement national example

The Recommendation suggests that measures include "processes to ensure access controls exist and are enforced". Further, "identifying products, services or suppliers that are considered potentially not secure are examples of possible risk mitigating measures."[22]

Member States should ensure that their national laws allow for effective risk mitigation measures. In France, for example, the Prime Minister issues a specific order (Fr: *arrêté*) listing equipment and technical devices that are subject to a risk assessment before being allowed onto the French market.[23] Moreover, a new French law is being proposed with a

[19] Item 14 of the Recommendation.
[20] Item 4 of the Recommendation refers to Directive 2002/21/EC and Directive 2002/20.
[21] Articles 13a and 13b of Directive 2002/21/EC and *inter alia* Annex, item 16 of Directive 2002/20. In Italy, for example, the Tender Rules for the award of the rights of use of radio frequencies in 5G, published by the Ministry of Economic Development in 2018, expressly provide for the successful tenderers' obligation to ensure the security of public networks against the unauthorized access according to the applicable national and European laws. See art. 10.6. Link: https://www.mise.gov.it/images/stories/normativa/Disciplinare_Gara_multibanda2018.pdf
[22] Item 15 (b) of the Recommendation.
[23] See the webside of ANSSI (*l'Agence nationale de la sécurité des systèmes d'information*) https://www.ssi.gouv.fr/actualite/publication-de-larrete-du-11-aout-2016-modifiant-celui-du-4-juillet-2012-fixant-la-liste-dappareils-et-de-dispositifs-techniques-prevue-par-larticle-226-3-du-code-penal/

similar procedure, but for 5G security in particular.[24] Violation of these laws may result in fines and imprisonment.[25] Italy has transposed Directive (EU) 2016/1148 (so-called NIS Directive) concerning measures for a high common level of security of network and information systems across the Union, by adopting a law - which is being implemented - applying to operators of essential services, including the digital infrastructures, and to suppliers of digital services. Such operators and suppliers must adopt technical and organizational measures that are appropriate and proportionate to the risks management and to prevent and mitigate the impact of accidents on network and information systems security.

### 3.3 Additional recommendations for national procedures and laws

Member States may consider the following:

1. Centralising the responsibility for risk assessments to one specialized designated authority, with powers to collect or request information for its assessments (see above regarding transparency).[26] Security assessments should be shielded from indirect political influence from foreign powers.

2. Ensuring legally binding effects of the outcome of a risk assessment, for example by empowering the authority to issue definitive decisions, e.g. through an authorisation, approval or declaration process. An authorisation could be subject to monitoring and reporting conditions, which incentivises compliance.

3. Decisions by the authority being subject to the same rights to appeal as in other similar areas of law if the national laws of the country so require.

4. Any legislation having proportionate sanctions for non-compliance, e.g. fines or other criminal sanctions, as well as making agreements void. [27]

## 4. Summary

| "Other" Factors | Example |
|---|---|

[24] Proposed new French rules in *code des postes et des communications électroniques* according to which the operators are responsible for the application for an authorisation, http://www.assemblee-nationale.fr/15/propositions/pion1722.asp.
[25] Article 226-3, of the Penal Code (Fr: *Code Pénal*).
[26] Compare: https://www.dni.gov/files/NCSC/documents/products/SCRM_Framework_for_Assessing_Risk_White_Paper.pdf.
[27] Draft law no. 1722 to protect national security and defence interests of France in relation to the operation of mobile networks, presented to the French National Assembly on 20 February 2019.

| | |
|---|---|
| Supplier's non-transparency | Supplier does not disclose information on ownership or financing. |
| Foreign state influence: ownership, control, financing, political influence over Supplier | Examples, state-owned companies, state funding, party representation or granting influence through a company's articles of association. |
| Conflict of laws and extraterritorial effect on Supplier | For example, the Chinese National Intelligence Law obliging a supplier or citizen in the EU to cooperate in intelligence gathering, breaching the right of confidential communication and GDPR rules. |
| Foreign regime's acceptance of the rule of law and separation of powers | Independence of judges and judicial system impact on the Supplier's means to challenge or oppose requests. |
| **Risk management measures/methods** | **Example** |
| Legal basis for Member States to act | For example, authorities should be able to impose conditions on operators when selecting Suppliers. |
| National procedures: centralised autonomous authority, binding decisions, right to appeal, enforcements through sanctions and fines | For example, an authority should be able to make risk assessments in relation to 5G products and services, and such assessments should become effective and operational through definitive decisions (e.g. an authorisation). A violation of the authorisation should lead to e.g. fines or personal liability. |