AVANCE
Insight 01/2021

Implementing the 5G toolbox: Could Finland serve as a model for the other EU countries?

Mikko **Alkio** & Petri **Rouvinen**

As a result of the European Commission's endorsement on 29 January 2020, the **toolbox** – a set of cybersecurity measures for the upcoming 5th generation of mobile telephony (5G) – became "soft law" in the EU. The member states were asked to hastily implement a vague piece of legislation and they were also pushed into making *de facto* trade policy that should be an exclusive responsibility of the EU. The issue was further complicated by a constitutional right-to-private-property dilemma embedded into the toolbox. It soon became evident that national implementations of the toolbox are quite diverse, which motivates our key question: *Is Finland a best practice case in this context and could it – at least in part – serve as a model for the other EU countries?*

On 7 December 2020, the Parliament of Finland approved a law allowing authorities to ban a network device on grounds of serious national security concerns. The law outlines an institutional setup isolating political and other aspirations from cybersecurity, which is seen as a technical matter. Even though the administrative process is collaborative and aggregates expertise of various stakeholders, power and responsibility resides with one authority (Traficom) that is also the foremost technical expert on the matter. The law confines administrative actions to the most central parts of the national infrastructure. It operates at the level of a device and does not permit banning "high risk vendors" outright. A process initiated by the authority can lead to the removal of a device, but only as a last resort. If so, the owner is entitled to a full compensation by the state.

The Finnish law provides a technology-neutral definition of critical infrastructure elements, which Traficom establishes with a working group consisting of various government authorities, telecom operators, major equipment providers, and other stakeholders. The list of the critical parts is based on 3GPP definitions and covers core network functions; it is noteworthy that the radio access network is not included in this list.

The Finnish model attends both to principles of good administration and to fundamental legal doctrines. The administrative process is transparent, and actions are grounded on objective evidence. In case of an unresolvable conflict, there is a path of legal recourse. All these feats are achieved with reasonably low administrative costs.

The Finnish implementation of the toolbox corresponds to what the ITU identifies as the final and the most desired stage of ICT regulation: it is collaborative, exploits synergies across sectors, and pools the expertise of diverse stakeholders. Other countries are well-advised to imitate these aspects of the Finnish implementation. There are, however, two preconditions for pursuing a similar solution: first, at least the responsible public agency must possess reasonably deep technical expertise; second, there must be sufficient willingness to cooperate among the involved public and private parties.

For the EU, tech sovereignty is unattainable[1]

Geopolitics and cybersecurity do not mix well – at least not in the current world, in which countries and regions/blocs simultaneously seek technological sovereignty but, in the case of technologically advanced products, utterly depend on geographically dispersed global supply chains.[2] On the positive side, interconnectedness via global supply chains (and specialization it implies) makes us more prosperous; on the negative side, it also makes us more vulnerable to foreign threats. Sovereign nations should certainly attend to their needs for national security, but they must also be aware of trade-offs they make in the process.

The United States and China might be able to move towards technology autonomy and even autarky; the European Union does not have such luxury – not even in the context of the upcoming fifth generation of mobile telephony (5G), despite of the fact that the EU happens to host two of the three globally leading 5G infrastructure providers – Ericsson (Sweden) and Nokia (Finland). Thus, in the ongoing "tech war" between the United States and China, the EU must carefully consider its options.

In the context of 5G, European public debate on perceived threats has been almost solely related to China. There is no reason, however, why European decisionmakers should view foreign threats asymmetrically.[3] Quite the contrary in fact: EU policies should be robust to threats regardless of their origin or type.

In this Avance Insight, we discuss the Finnish implementation of the 5G toolbox of the European Commission. The question we pose to ourselves is as follows: *Is Finland a "best practice" case in this context and could it – at least in part – serve as a model for the other EU countries to follow?*

Cybersecurity is paramount in the context of 5G

5G is still in its early days – even in Finland serving as a testbed for it. The turn of the year 2020–2021 nevertheless defined a critical junction in the evolution of 5G, as its rollouts are soon to be put to higher gears in most advanced countries.

5G is evolutionary in the sense of being based on earlier generations of mobile telephony and on digital infrastructure more generally. It is also revolutionary in a few aspects. Unlike the previous generations of mobile networks, 5G is built with autonomous and automated machine-to-machine communication as a key priority; furthermore, 5G can present different virtualizations of itself depending on the needs of applications riding on it. Otherwise, 5G promises a combination of unprecedentedly high data transfer speed/volume and low delay in data transfer (latency). These features, along with the support for low power connections, are envisioned to bring mobile connectivity to billions of Internet-of-Things (IoT) devices ranging from mining equipment to transmitters in clothing. With the technology's ever-deeper integration into our lives, cybersecurity in 5G is paramount.

To achieve the afore-mentioned feats, 5G uses multiple spectrum frequencies and requires smaller cells (implying densely located base stations), which in turn imposes new requirements on fiber-optic infrastructure and further fosters the convergence of mobile and fixed communications networks. It has been suggested that the small cell size and other technical requirements make 5G the biggest technology investment in human history. Thus, it matters a great deal, what are the regulatory conditions – and by extension competitive landscapes – covering 5G rollouts.

[1] Huawei Technologies Oy (Finland) Co. Ltd is a client of Avance Attorneys Ltd. Avance is solely responsible for the content of this report.

[2] In debating the issue, a briefing by the European Process Safety Centre (EPSC is a part of the European Commission) notes (p. 10; the emphases as in the original): "… in today's interconnected world of globalised supply chains, no one can walk alone. From a strategic point of view, the issue is hence **more complex than simply seeking to prevent, or eliminate, vulnerabilities in supply chains**. In many respects, it appears more realistic to find ways to **manage and reduce, when possible, these vulnerabilities**."

[3] At least in some parts of the EU, also espionage by the United States is viewed with suspicion. For example, the US Cloud Act, which grants US authorities access to data hosted by American companies anywhere in the world, motivated the EU – with the endorsement of France and Germany – to launch its Gaia-X project.

The broader context of 5G policymaking in an EU country

As the previous section on the characteristics of 5G suggests, this infrastructure integrates deeply into all walks of life. The same is true for 5G-related politics and regulation: decisions that ultimately matter to citizens – both individuals and companies – relate to *conditions imposed on private companies that operate 5G networks and that contract other private companies for network build-up, maintenance, and other supporting services*. These day-to-day business decisions take place in a broad global context and have society-wide implications. For 5G investments to take place at all, there must be a reasonable understanding of the future business environment – starting with fundamental issues such as respect for private property and ending with minute details of how the infrastructure can be built and maintained.

Figure 1 illustrates the broader international context: The EU should pass laws and directives as well as make policies and regulations that are in line with international conventions and agreements it has pledged to follow. The member states are obliged to implement EU laws and regulations, even though they are – at times deliberately, in order to adapt to national idiosyncrasies – left with some room to maneuver. In the context of 5G, it is undeniably the member states that oversee security requirements imposed on communications service providers and decide on practical details.

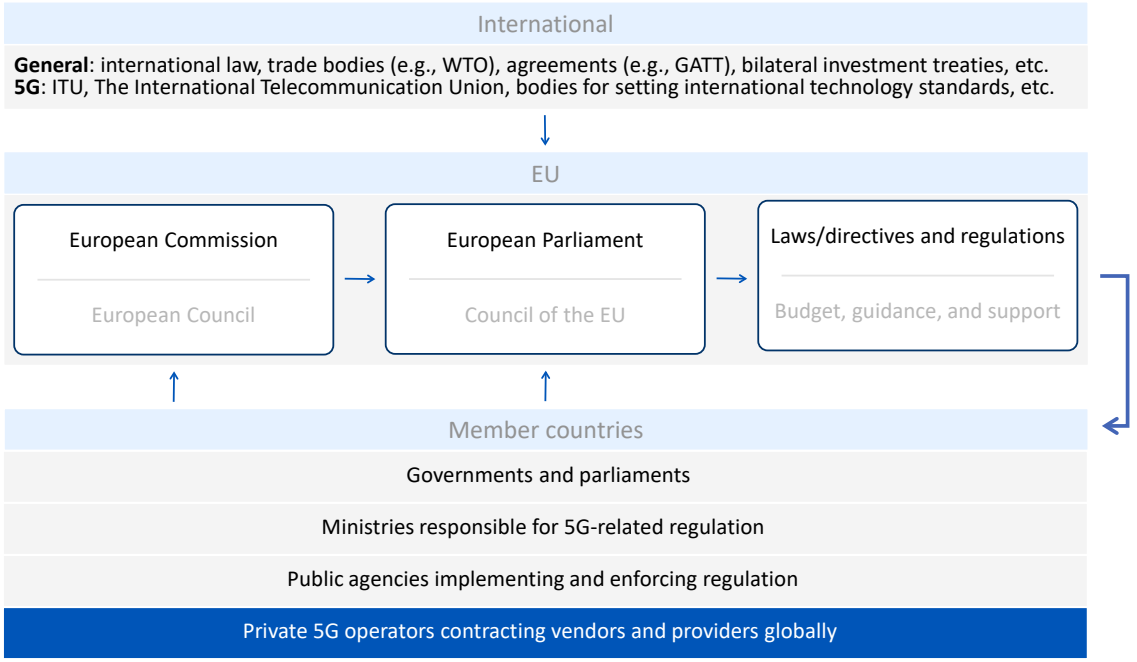

Figure 1: The global context of making 5G-related decisions in an EU country – what ultimately matters the most are conditions imposed on private companies building, owning, and operating 5G networks.
Source: The authors.

While there are time-honored principles of good public governance in relation to Figure 1, there is little that would directly guide us in thinking of 5G regulation. One exception is a large body of work done by ITU, The International Telecommunication Union,[4] over several decades, in which five generations of ICT regulation are recognized. On the final stage – co-incidentally labelled G5, without a direct link to 5G – ITU notes (the emphases added):[5]

> "G5 regulation, **collaborative** regulation, is the desired destination for regulation at this point in time and one that can drive ICT markets globally on the way to digital transformation. It is different from G4 regulation in the means it uses and the mechanisms that have been put in place to increase **synergies across the sectors** and create **efficiencies across public administration bodies**."

[4] The United Nations specialized agency for information and communication technologies, https://www.itu.int.

[5] https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Policy-&-Regulatory-Frameworks.aspx, visited 21 Jan. 2021.

The EU 5G toolbox outlines the principles for the member states' actions

On 29 March 2019, the European Commission published a recommendation on the cybersecurity of 5G networks.[6] Subsequent developments led to the Commission's adoption of a communication on the Secure 5G deployment,[7] with a simultaneous publication of a 5G toolbox,[8] on 29 January 2020. In its communication, the Commission notes that

> "While Member States will decide on the suitability of a particular measure based on national circumstances, it is absolutely essential that a set of key measures... is put in place in every Member State..."

In reference to equipment vendors, the Commission states that

> "The assessment of the risk profiles of suppliers should be conducted solely on security grounds and based on objective criteria."

From a member state's vantage, on 29 January 2020 the 5G toolbox became "soft law" that should be implemented nationally. In tandem with the Commission, the Finnish Ministry of Transport and Communications issued a press release noting that:[9]

> "In Finland, the preparations were made in extensive cooperation between the authorities led by the Ministry of Transport and Communications.
>
> Member States will review the contents of the Toolbox and assess whether changes to national legislation, for example, are needed. The Finnish Transport and Communications Agency (Traficom) supports network operators and equipment manufacturers in using the Toolbox.
>
> In Finland, potential needs for legislative changes will be identified and amendments implemented as part of law drafting work."

The Toolbox identifies strategic and technical measures as well as supporting actions the member states should implement; these are summarized in Appendix 1. A glance at the measures in the toolbox reveals that they are quite generic – rather than being a cookbook with step-by-step instructions (as its name would suggest), the toolbox outlines a set of guiding principles and thus leaves it to each member state to choose an appropriate course of action.

The EU toolbox has put the member states in a difficult situation:

- First, the toolbox has not been prepared in the same manner as EU directives and does not meet the usual standards of EU law. Even though the toolbox is rather vague (and even internally inconsistent on occasion), the member states have been requested to implement it at an unusually rapid pace.
- Second, the Treaty of the Functioning of the European Union[10] defines trade policy as an exclusive responsibility of the EU[11] but – in the context of the toolbox – national governments of member states are left to decide on matters impacting international trade of 5G infrastructure equipment.
- Third, the toolbox entails a difficult constitutional dilemma regarding the right to property, which was exposed and debated in Finland (we further elaborate on the issue upon discussing the Finnish implementation of the toolbox).

---

[6] Recommendation (EU) 2019/534 on the cybersecurity of 5G networks, Official Journal of the European Union L 88, 29 March 2019, pp. 42–47, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=EN.

[7] European Commission, Brussels 29 January 2020, COM(2020) 50 final, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: *Secure 5G deployment in the EU - Implementing the EU toolbox*, https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-50-F1-EN-MAIN-PART-1.PDF .

[8] The NIS Cooperation Group, *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*, CG Publication 01/2020, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[9] Ministry of Transport and Communications (Finland), 29 January 2020 at 14:45 (local time), *Ministry Security of 5G networks improve through coordinated European approaches*, https://valtioneuvosto.fi/en/-/euroopan-yhteiset-linjaukset-lisaavat-5g-verkkojen-turvallisuutta.

[10] *Article 3 of the Treaty of the Functioning of the European Union* (TFEU), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12016E003.

[11] https://ec.europa.eu/trade/policy/policy-making/.

Although the European Commission has called for EU-wide coordination in the context of the toolbox, it has taken – most likely unintendedly – the afore-mentioned steps leading to diverging national implementations, as the Commission has learned in both of its own reviews and in the one by the European Court of Auditors.[12] Indeed, this divergence motivates our search for best practices in implementing the toolbox.

Implementation of the toolbox in Finland [13]

On 7 December 2020, the Parliament of Finland (Eduskunta) approved a law allowing authorities to ban telecommunications network equipment, if its use seriously endangers national security or defense.[14] The law states that (emphasis added)[15]

> "A communications network **device** shall not be used in critical parts of a public communications network if there are weighty grounds to suspect that the use of such device endangers national security or defence..."

Therefore, the Finnish law focuses on the security of a specific network device; it neither assesses suppliers as a whole nor labels any as a high-risk vendor. On 19 May 2021, Traficom – in close collaboration with industry participants – provided a technology-neutral and supplier-independent list of the critical elements;[16] it is noteworthy that the radio access network is not among the list of critical components.

The law introduces a new institutional arrangement (emphasis added):[17]

> "A new **advisory board for network security** will be set up to monitor the security of communications networks. The advisory board will consist of representatives of the telecommunications industry and the central authorities from different administrative branches. The advisory board will discuss extensively questions related to the security of communications networks and, if necessary, issue recommendations for the improvement of network security."

Several further details are noteworthy in the Finnish law:

- Finland neither banned vendors based on the country of origin nor singled out any.
- The Finnish law only applies to the most critical parts of the network – understood as the most central nodes of network traffic.
- The law states that if the authority ordered network gear to be removed, the government would pay full compensation.

As Minister of Transport and Communications Timo Harakka has noted,[18] Finland has systematically attended to the security of the national communications infrastructure since the 1990s. Thus, for Finland the new legislation is simply a further incremental step on a path traced decades ago.

---

[12] Samuel Stolton (EURACTIV.com 8 Jan. 2021, updated 25 Jan. 2021), *EU nations divided on 5G security, auditors say*, https://www.euractiv.com/section/5g/news/eu-nations-divided-on-5g-security-auditors-say/ (visited 28 Jan. 2021).

[13] The law covers a wider range of issues, as the press release by the Ministry of Transport and Communications (Finland) on 30 Dec. 2020 at 14:14 notes (*Act on Electronic Communications Services enters into force on 1 January 2021*, https://valtioneuvosto.fi/en/-/act-on-electronic-communications-services-enters-into-force-on-1-january-2021) : "The reform will implement the requirements of the EU Directive on Audiovisual Media Services (so-called AVMS Directive) and the European Electronic Communications Code (so-called Telecoms Package Directive). It will also put into place measures included in the common toolbox to secure the EU's 5G networks to protect critical parts of the communications network."

[14] https://finlex.fi/fi/esitykset/he/2020/20200098.

[15] SVPL 244a§: "Viestintäverkkolaitetta ei saa käyttää yleisen viestintäverkon kriittisissä osissa, jos on painavia perusteita epäillä, että laitteen käyttäminen vaarantaisi kansallista turvallisuutta tai maanpuolustusta siten, että käytöllä mahdollistettaisiin ulkomainen tiedustelutoiminta tai toiminta, jolla häirittäisiin, lamautettaisiin tai muuten vahingollisella tavalla vaikutettaisiin Suomen tärkeisiin etuihin, yhteiskunnan perustoimintoihin tai kansanvaltaiseen yhteiskuntajärjestykseen."

[16] On 19 May 2021, Traficom defined the critical parts of network infrastructures (19.05.2021 TRAFICOM/161584/03.04.05.00/2020; https://www.finlex.fi/fi/viranomaiset/normi/480001/47015). For 5G, Traficom's listed critical parts is as follows: Access and Mobility Management Function (AMF), User Plane Function (UPF), Policy Control Function (PCF), Authentication Server Function (AUSF), Unified Data Management (UDM), Application Function (AF), Network Exposure Function (NEF) and Intermediate NEF (I-NEF), Network Repository Function (NRF), Network Slice Selection Function (NSSF), Network Slice Specific Authentication and Authorization Function (NSSAAF), Session Management Function (SMF), Security Edge Protection Proxy (SEPP), Unstructured Data Storage Function (UDSF), Unified Data Repository (UDR), UE radio Capability Management Function (UCMF), Non-3GPP InterWorking Function (N3IWF), 5G-Equipment Identity Register (5GEIR), Service Communication Proxy (SCP), Service Communication Proxy (SCP), and Network Data Analytics Function (NWDAF; excluding certain functionalities).

[17] https://www.lvm.fi/-/act-on-electronic-communications-services-enters-into-force-on-1-january-2021-1250443.

[18] https://yle.fi/uutiset/3-11607121.

Traficom, the Finnish Transport and Communications Agency, oversees defining practical elements relevant to the law and its enforcement. As the above quote indicates, Traficom's work is supported by the advisory board for network security (Verkkoturvallisuuden neuvottelukunta) with a representation of multiple stakeholders.

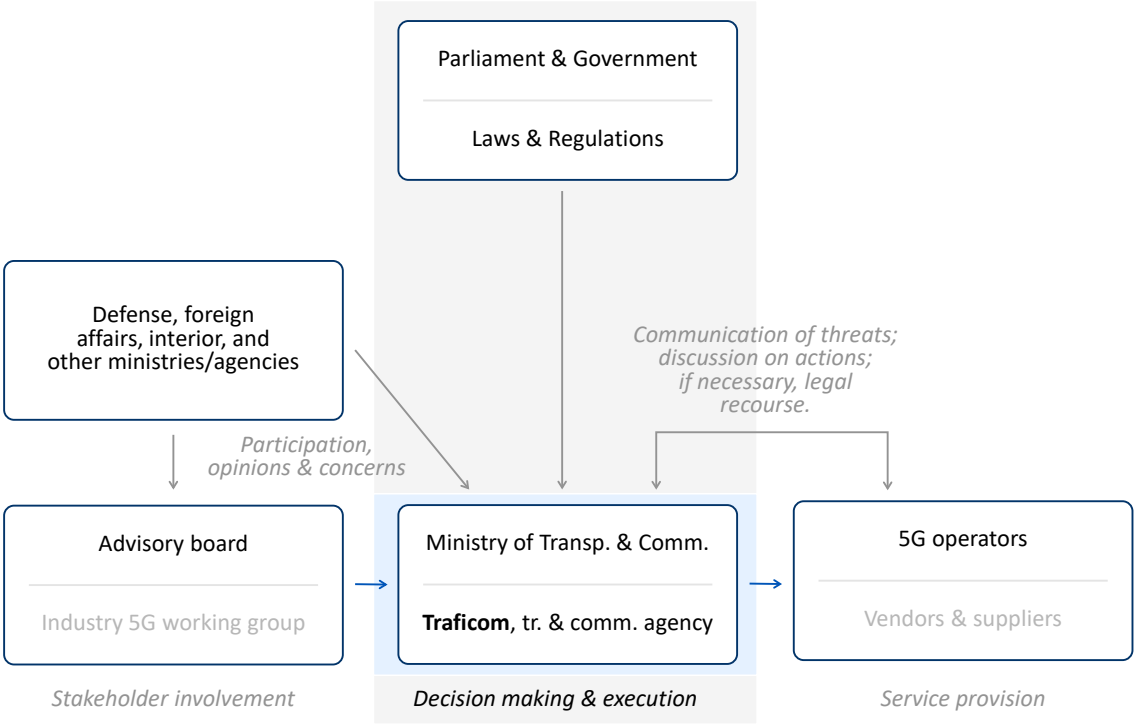

Figure 2: The 5G toolbox implementation framework in Finland – the process involves all relevant stakeholders, but the decision-making power and responsibility resides with Traficom.
Source: The authors.

Figure 2 illustrates the broader administrative context of the law. As said, day-to-day execution resides at Traficom (and the Ministry of Transport and Communication above it). All other public bodies may express concerns and opinions to Traficom (the most important ones also via the advisory board), but *per se* they are not decisionmakers. Traficom consults operators and other stakeholders via the advisory group and via a technical working group that has both operators and equipment vendors among its members; among other things, debates in these two groups relate to how critical a given type of equipment is, how serious a perceived threat to national security is, and in what viable ways a potential threat can be diffused.

If Traficom suspects that a device constitutes a security threat, it first informs the applicable operator. The operator must be heard, and it must be given a possibility to remedy the security issue Traficom has identified (such remedy could be, e.g., a software update). Only as the last resort, Traficom can require the operator to remove the device. If so, according to the law, the State of Finland shall provide the operator full compensation for all direct costs and losses.

The implementation of the toolbox involved discussion on certain constitutional issues relating to the protection of private property. In this respect, it is noteworthy that Finland does not have a constitutional court conducting *ex post* legal review, but the constitutionality of new laws is instead evaluated *ex ante* by the Finnish Parliament's Constitutional Law Committee (CLC). In its statement regarding the Government's legislative proposal, *the CLC found that the prohibition of using a device and the requirement of having it removed from the network essentially equated with the expropriation of private property*. According to the CLC, this is the case both for equipment that has already been installed when the legislation including said prohibition is enacted but also for equipment that is installed subsequently, to the extent such equipment's owner cannot have been aware of the weighty grounds to suspect that the equipment's use endangers national security or defense when making its investment decision.[19] Consequently, and as the Finnish Constitution requires full compensation to the owner in case of expropriation of private property, the new

[19] Statement by the CLC (PeVL 35/2020).

legislation includes a provision whereby the network operator is entitled to full compensation payable by the State in both of the above scenarios. The compensation payable covers the actual costs of removing and replacing the device as well as other financial losses, such as labor, repair and alteration costs, and the cost of purchasing a replacement device. Compensation is also paid for other immediate financial losses, if any.

To summarize, the core features of the Finnish implementation are as follows:

- Administrative execution resides with Traficom that – among public bodies in Finland – has the deepest and longest expertise in 5G-related technical matters. In judging technical aspects and in determining potential threats, Traficom has several channels to access diverse expertise and views of all stakeholders in Finland.

- Traficom must operate at the level of a device in identifying security threats, which have to be objectively verifiable. Once Traficom proceeds, the operator in question must be heard and it must be able to propose a remedy. Only as a last resort, Traficom can order a removal of a device, in which case the operator is entitled to full compensation by the state. If the operator (or another immediate stakeholder) is unhappy with the outcome, it has a right to appeal.

Conclusions

The Finnish implementation of the toolbox corresponds to what the ITU identifies as the final and the most desired stage of regulation, G5 (as discussed in the introduction, without any direct link to 5G): it is collaborative, exploits synergies across sectors, and pools expertise of diverse stakeholders. Indeed, Finland has a long tradition of productive public-private cooperation, which is one of the central elements of the Nordic welfare society model.

Despite the collaborative nature of the process, power and responsibility resides in one place – Traficom – that also has the deepest technical expertise on the matter. Indeed, one might go as far as arguing that having sufficient expertise in the public administration is a precondition for the kind of implementation Finland has chosen for itself.

The Finnish model attends both to principles of good administration (such as proportionality and objectivity) and to fundamental legal doctrines (such as the protection of property and freedom of expression). The administrative process is fully transparent, and actions are grounded on objective and verifiable criteria. There is no tolerance for argumentation or reasoning that would not be exposed to public scrutiny. If the collaborative apparatus yielded an otherwise unresolvable controversy, there would be a clear path of legal recourse.

In the Finnish law, cybersecurity is seen as a technical issue that needs a technical solution. Political aspirations or other aspects of public administration are kept separate. The law confines administrative actions to the most central parts of the national infrastructure, which limits its scope and curbs administrative costs.

The Finnish law operates at the level of a device; it does not permit banning "high risk vendors" outright. It has been suggested that this goes against certain measures of the toolbox; in our interpretation, however, the toolbox does *not* leave scope for excluding vendors merely based on geopolitical criteria. Furthermore, the Finnish procedure does *not* exclude viewing *all* gear by a certain vendor with suspicion.

While the Finnish model has many virtues and it is to be commended, it does have two somewhat constraining prerequisites: (1.) relatively high level of technical expertise in the administration and (2.) willingness of other administrative branches and private parties to cooperate. If these are in place, aspects of the Finnish model are well worthy of a consideration also in the other EU countries.

Appendix 1: Measures and supporting actions in the 5G toolbox

Source: **The NIS Cooperation Group**, *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*, CG Publication 01/2020, pp. 11–13, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

4.1.1 Strategic measures cover measures concerning increased regulatory powers for authorities to scrutinise network procurement and deployment, specific measures to address risks related to non-technical vulnerabilities (e.g. risk of interference by a third country or dependency risks), as well as possible initiatives to promote a sustainable and diverse 5G supply and value chain in order to avoid systemic, long-term dependency risks. Strategic measures are potentially highly effective in addressing certain 5G cybersecurity risks identified in the EU coordinated risk assessment report.

The following eight strategic measures have been identified:

- SM01 Strengthening the role of national authorities;
- SM02 Performing audits on operators and requiring information;
- 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;
- SM04 Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support;
- SM05 Ensuring the diversity of suppliers for individual MNOs through appropriate multivendor strategies;
- SM06 Strengthening the resilience at national level;
- SM07 Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU;
- SM08 Maintaining and building diversity and EU capacities in future network technologies.

4.1.2 Technical measures include measures to strengthen the security of 5G networks and equipment by reinforcing the security of technologies, processes, people and physical factors. The effectiveness of the technical measures in terms of risk mitigation will vary depending on the scope of the measures and on the types of risks to be addressed. In particular, technical measures alone would not allow to address non-technical vulnerabilities (e.g. risk of interference by a third country or dependency risks).

The following 11 technical measures have been identified:

- TM01 Ensuring the application of baseline security requirements (secure network design and architecture);
- TM02 Ensuring and evaluating the implementation of security measures in existing 5G standards;
- TM03 Ensuring strict access controls;
- TM04 Increasing the security of virtualised network functions;
- TM05 Ensuring secure 5G network management, operation and monitoring;
- TM06 Reinforcing physical security;
- TM07 Reinforcing software integrity, update and patch management;
- TM08 Raising the security standards in suppliers' processes through robust procurement conditions;
- TM09 Using EU certification for 5G network components, customer equipment and/or suppliers' processes;
- TM10 Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services);
- TM11 Reinforcing resilience and continuity plans.

4.1.3 In addition, a set of targeted supporting actions have the potential to enable and assist the strategic and technical measures and thereby enhance their effectiveness:

- SA01 Reviewing or developing guidelines and best practices on network security;
- SA02 Reinforcing testing and auditing capabilities at national and EU level;
- SA03 Supporting and shaping 5G standardisation;
- SA04 Developing guidance on the implementation of security measures in existing 5G standards;
- SA05 Ensuring the application of standard technical and organisational security measures through specific EU-wide certification scheme;
- SA06 Exchanging best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers;
- SA07 Improving coordination in incident response and crisis management;
- SA08 Conducting audits of interdependencies between 5G networks and other critical services;
- SA09 Enhancing cooperation, coordination and information sharing mechanisms;
- SA10 Ensuring 5G deployment projects supported with public funding take into account cybersecurity risks