Kadri Katariina Johanson
Aethra Marie Raabe
Merilin Teppo

METHODS OF REGULATING ACCESS
TO THE TELECOMMUNICATIONS MARKET
FOR REASONS OF NATIONAL SECURITY

IT Law Lab

Tartu
2020
Table of contents

INTRODUCTION ......................................................................................................................... 3

1. Overview of Threats and Current Legal Framework .......................................................... 6
   1.1. Threats to National Security ......................................................................................... 6
   1.2. EU Company vs Third-Country Company ................................................................. 7
   1.3. Existing Legal Framework ......................................................................................... 8

2. Analysis of the Proposed Legislation and its Refusal by the Ministry of Justice .............. 11
   2.1. Amendments Proposed by the Ministry of Economic Affairs and Communications.... 11
   2.2. Issues Related to the Refusal by the Ministry of Justice ........................................... 12

3. Legal solution ................................................................................................................................. 19
   3.1. Solutions from Other Member States .......................................................................... 19
   3.2. Amendments to the Electronic Communications Act ................................................. 21
      3.2.1. The Power to Establish a Verification Procedure .................................................... 21
      3.2.2. Amendments to the Regulation of June 22, 2016 No. 140 “Requirements for provision of communications services and technical requirements for communications networks” ...................................................................................................................... 22

SUMMARY ................................................................................................................................... 29

BIBLIOGRAPHY ......................................................................................................................... 31

APPENDIX 1 ................................................................................................................................. 34
INTRODUCTION

Telecommunications industry has significantly changed people's lives in the last two decades, and recent telecommunications rules have contributed to transform the telecoms landscape from monopolies to a competitive market with a wide range of offers. Telecommunications networks are regulated on a national level within state borders, meaning states are facing new challenges and potential consequences with the arrival of new technologies. It is particularly relevant while stepping into an era of 5G mobile and wireless communications technology.

Whereas the European Union supports Digital Single Market and has a vision to create a Gigabit Society, open telecommunications markets in the Member States are expected, resulting in the drive of digital economic development and competitive prices for the end-users.

On the other hand, the Member States like Estonia have critical sectors dependent on information and communication technologies (ICT), meaning telecommunications companies with possible vulnerabilities in its technologies or even ulterior motives might have capabilities to pose a threat to national security. The purpose of the Estonian security policies is to ensure Estonia’s independence and freedom, territorial integrity, constitutional regime, and the security of the population. According to the Ministry of Defence, national defense is described as a collection of broad-based activities, including the continuity of operation of vital services. Consequently, appropriate measures should be taken to avoid any threats to national security.

As the description of the current IT Law Lab has indicated, a legal solution should be offered how Estonia could prohibit a company entering its telecommunications market when consisting a threat to its national security. These companies are seen as entities who provide communications services to end-users by themselves or with the help of third parties, e.g. suppliers such as telecom equipment manufacturers.

---

In this work telecommunications company or telecommunications undertaking refers to a provider of publicly available electronic communications services. In particular, service providers whose services are consumed by at least 10,000 end-users and who provide vital services, e.g. the phone, mobile phone and data transmission services.

Based on the hypothesis that there is a potential threat in the form of malicious companies who wish to enter the Estonian telecommunications market with an ulterior motive, authors of this work will try to indicate the options for the state to restrict such companies from entering the market. In the light of the current security situation and technological developments, the work will provide analysis of different aspects of whether and how could Estonia prohibit a European company and/or a third-country company from entering the Estonian telecommunications market.

The authors have taken into account the recommendation of the consulting entity, the Ministry of Economic Affairs and Communications, narrowing the focus of the analysis in the prism of the recent amendment to the regulation “Requirements for provision of communications services and technical requirements for communications networks” regarding two specific paragraphs. The work will also offer additional proposals how to regulate access to the telecommunications market for reasons of national security.

The importance of the topic derives from the fact that currently the access to the telecommunications market for reasons for national security are not regulated in Estonia. The Ministry of Economic Affairs and Communications is dealing with the legal challenges of implementing necessary legal grounds for assessing possible national threats and options of Estonia to restrict companies with malicious intent or whose network infrastructure might include unreliable or even malicious technology.

The first chapter of the work gives an overview of the threats and the telecommunications market access, taking into account current existing legal framework. The second chapter analyses the proposed legislation by the Ministry of Economic Affairs and Communications taking into account the corresponding refusal to approve it by the Ministry of Justice. In the

5 Estonian telecommunications companies, e.g. Telia Eesti AS, Tele2 Eesti AS or Elisa Eesti AS.
6 Definition corresponds to the definition of service providers in Electronic Communications Act art 87(4).
third chapter, additional proposals are given how to regulate access to the telecommunications market for reasons of national security.

Acknowledgements

The authors would like to thank Anna-Liisa Pärnalaas and Sten Tikerpe from the Ministry of Economic Affairs for their assistance in defining the scope of the work as well as their valuable suggestions.

Overview of the contribution:

All members participated in Skype calls and written conversations where problems and possible solutions were discussed and analysed. All members participated in a conference call via Skype with Anna-Liisa Pärnalaas and Sten Tikerpe from the Ministry of Economic Affairs.

In chapter 1, the first part was mainly written by Merilin Teppo, the second part by Kadri Katariina Johanson and the third by Aethra Marie Raabe. The rest of the work was written by all members together, through active discussion with regards to the solutions presented.

Keywords: telecommunications, 5G, telecommunications market access, network infrastructure, national security.
1. Overview of Threats and Current Legal Framework

1.1. Threats to National Security

Telecommunications technology refers to distance communications, such as radio, telephone, television, satellite, data communication and computer networking. The main components of a telecommunications system are:

1. the transmitter, a device that originates communication, e.g. cell tower.
2. the transmission medium, the medium over which the transmission takes place, e.g. atmosphere or cable and
3. the receiver, the end point of the transmission, e.g. radio receiver (simply radio) and cell phone.

All of these components can be simplified into software and hardware.

Telecommunications infrastructure that provides the necessary backbone for information exchange have been found to be particularly vulnerable to various forms of attacks. Estonia has built a digital society where 99% of public services are available via the Internet as e-services, therefore Estonia should be highly concerned about the threats of allowing any malicious company or company that has malicious network infrastructure elements to gain power inside Estonian telecommunications networks. It is therefore important to assess threats related to these companies and thus, various forms of threats to national security are firstly defined.

Firstly, threats to national security in terms of telecommunications availability may occur when the servers are not up anymore and network communication stops working due to an unauthorized activity. For example, when a telecommunications company or a supplier of the telecommunications company (hereinafter attacker) with ulterior motives takes advantage of the weakness of the network components, e.g. cell tower and shuts down the tower or disrupts

---

8 Telecommunications Technology. ACE Electoral Knowledge Network. Online: http://aceproject.org/ace-en/topics/et/eta/eta01/default (03.01.2020).
9 Ibid.
some important Estonian network traffic then this can be a threat to national security. Furthermore, companies may put malicious hardware or software components inside their equipment that can be used to paralyze equipment to collapse communication system.

Secondly, threats to national security in terms of telecommunications integrity may occur when an attacker takes advantage of the weakness of the network components and tampers the communications contents, e.g. spreads propaganda or changes the data while in transit.

Thirdly, threats to national security in terms of telecommunications confidentiality may occur when an attacker takes advantage of the weakness of the network components and listens to the network traffic. The attacker could also look on the data stream and on the storage for purposes like espionage, both corporate and governmental. Moreover, companies’ hardware could provide a backdoor for some other state surveillance apparatus.

Therefore, affecting the network infrastructure components may potentially compromise the availability, integrity and confidentiality of the network services, and consequently be a threat to national security.

1.2. EU Company vs Third-Country Company

Telecommunications companies are subject to European Union and the Member States’ national law when providing services in the EU, more specifically subject to a legal framework of establishing conditions of electronic communications networks or services, and specific requirements, that national authorities have the authority to impose. Telecommunications companies in the EU differ in aspects like market positioning, ownership and strategies in regards to the use of suppliers for their equipment and services. As an example, some are using and running their networks by different equipment suppliers while others are devoted to one. And even though the European companies show a sufficient level of


transparency, a chance that key network functions will be managed by such subcontractors, located in a different state, possibly outside the EU prevails.\textsuperscript{17} Moreover, the shift to software-based networks and their virtualisation may contribute to the key network functions being managed by such subcontractors, most probably located in a different Member State than the mobile network operator or even in a third country.\textsuperscript{18} Therefore, legal solutions of how Estonia could prohibit a European company and a third-country company from entering the Estonian telecommunications market for reasons of national security shall be laid out.

Taking into consideration that there is currently no unified approach by the Member States to assess national security threats, as laid out further in chapter 3 of the work, the authors believe a unified approach should be taken in the legislation to both, EU companies and third-country companies when considering the threat they pose to national security. The fact that one company might already be operating in another EU Member State, may not guarantee that they meet the level of security the Estonian government would require from them. Therefore, it is questionable whether there is a reason to treat third-country companies differently from companies already operating in the EU. Additionally, the offered legal solution should help to ensure that the telecommunications company receives a permit or refusal before the planned investment.

**1.3. Existing Legal Framework**

Under the EU telecommunications framework, obligations can be imposed on telecommunications operators by the relevant Member State(s) in which it is providing service.\textsuperscript{19} Under the Telecoms Regulatory Framework (Article 13a of Directive 2002/21/EC as amended by Directive 2009/140/EC), Member States are required to ensure that telecoms operators: a) take appropriate measures to manage security risks and b) take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks. The Electronic Communications Code (Directive 2018/1972), which replaces the Telecoms Regulatory Framework and must be transposed by the Member States by 21 December 2020, contains similar provisions.

The European Commission has stated in its Recommendation that a Member State has competence and right to exclude providers or suppliers from their markets for national security

\textsuperscript{17} Ibid, p 10.
\textsuperscript{19} Ibid, p 29.
Pursuant to Article 4 (2) of the Treaty of the European Union, EU law, including the Charter of Fundamental Rights of the European Union, shall not apply to matters regarding the national security of the Member States.

Currently, the entrance to telecommunications market in Estonia is regulated in the Electronic Communications Act. According to clause 2 5) of the Electronic Communications Act electronic communications undertaking means a person who provides publicly available electronic communications services to the end-user or to another provider of publicly available electronic communications services.

For illustrative purposes the requirements for the provision of telecommunications services in Estonia pursuant to Electronic Communications Act are outlined. According to subsection 3 (1) and subsection 4 (1) of the Electronic Communications Act each person who wants an entry to the Estonian market has the right to commence the provision of communications services, and for the provision of communications services a notice of economic activities must be submitted. In addition, according to the provisions of the General Part of the Economic Activities Code Act, a notice of economic activities shall set out a description of the provided communications service and the geographical area of the activity. Requirements for provision of communications services and communications networks are found from chapter 8 of the Electronic Communications Act.

The requirements for provision of communications services and communications networks related to national security mainly come from section 87. Specifically clause 87 (1) 9) of the Act states that communications undertakings shall be guided by ensuring public order and national security and clause 87 (2) 4) of the Act further states that the Government of the Republic may establish technical requirements for the communications networks and requirements for the provision of communications services if this is necessary for ensuring public order and national security.

However, while this gives the government the right to establish technical requirements for ensuring public order and national security, there is currently no regulation that actually further establishes any such requirements or otherwise expands on that right. There is regulation for

---


22 Electronic Communications Act subsection 4 (2).
other requirements for provision of communications services and communications networks, but there is no existing regulation to allow any national risk assessment *ex ante* and prohibit companies from entering the telecommunications market based on a threat to national security. Moreover, there is no regulation to prevent existing companies from implementing malicious network infrastructure components.

Consequently, if the state would like to use the basis from current clause 87 (2) 4) of the Act to prohibit companies that pose a threat to national security from entering the Estonian market, an appropriate regulation would be needed to be altered or new one adopted, taking into account authorization limits and fundamental rights.

---

2. Analysis of the Proposed Legislation and its Refusal by the Ministry of Justice

2.1. Amendments Proposed by the Ministry of Economic Affairs and Communications

An ICT equipment trust policy working group was formed in Estonia on 26.06.2019 by the Minister for Foreign Trade and Information Technology upon rescript No.1.1-1/19-100. The working group was formed by representatives from different ministries and public authorities who analyzed the risks of Estonian national telecommunications market in the light of the current security situation and the potential technological developments. As a result, a regulation draft/project was formed and presented by the Minister for Foreign Trade and Information Technology and the Ministry of Economic Affairs and Communications to the Ministry of Justice on the 15.11.2019. The aim was not to amend the Electronic Communications Act, but based on clause 87 (2) 4) of the Act and the principles and objectives of subsection 87 (1) of the Act, to make an amendment to the regulation “Requirements for provision of communications services and technical requirements for communications networks” regarding two paragraphs.24

Namely, the draft suggested to supplement subsection 3 (1) of the regulation with a new clause 11, a general norm to require the provider to plan, design, build, maintain and use communications networks in such a way which would be compatible with the state’s national security interests.25 The second amendment included adding a new paragraph, section 31 to the regulation with five subsections. The new paragraph would require the companies to provide Consumer Protection and Technical Regulatory Authority with technical documentation before starting to use new hardware and software. The technical documentation would be required to contain at least the following about the hardware and software: the name, the company that produced it, the function in the communications network, the place of use in the communications network and the beginning and end date of use. This information would be relayed to the security authorities and the Information System Authority, and when necessary, to the Cyber Security Council of the Security Committee of the Government for their opinion.

The following amendments were proposed to allow any national risk assessment ex ante to prohibit companies from entering the telecommunications market based on a threat to national security. The explanatory note of the proposed draft stated that during its preparation various

25 Ibid.
options were considered to ensure the compatibility of communications networks with the national security interests. For that reason, the given solution was chosen to ensure that the communications company would receive a permit or refusal from the state before the planned investment in the network would be completed.\textsuperscript{26}

2.2. Issues Related to the Refusal by the Ministry of Justice

Undoubtedly, the proposed legislation has set forth possible solutions for relevant concerns regarding the ICT infrastructure and the compatibility of communications networks with the national security interests. However, the presented draft contains contradictions and issues that in the present case have caused the Ministry of Justice to reject the draft, as laid out in the official reasoning provided on 23.12.2019. In this section the issues that the Ministry of Justice laid out, will be examined and possible solutions will be offered to make the draft acceptable and efficient for its purpose.

1) The Ministry of Justice has stated that an \textit{ex-ante} assessment, whether a company is permitted to operate on the telecommunications market or not, is infringing the freedom of enterprise according to section 31 of the Estonian Constitution, and thus making the regulation not constitutional.\textsuperscript{27} Hereby, it would be important to analyze whether the conclusion is solid and whether such infringement would be justified.

For such conclusion different aspects should be examined and an analysis of the constitutionality of the methodology applied by the Constitutional Review Chamber of the Supreme Court and the Chancellor of Justice should be carried through. Infringement as such is a phenomenon that often occurs, whereas the concern is in its proportionality. Therefore, two questions should be raised - does the proposed legislation have a legitimate aim, and does it outweigh the infringement of the freedom of enterprise?\textsuperscript{28}

Considering that the main purpose of the proposed draft is creating telecommunications market conditions to ensure public order and national security, it is evident that the

\textsuperscript{26} Eelnõu 14.11.2019 Vabariigi Valitsuse 22. juuni 2006. a määruse nr 140 „Nõuded sideteenuse osutamisele ja sidevõrkude tehniliseks nõudeks“ muutmine.
The proposal stands for compelling state interest. Taking into account that the ICT infrastructure in Estonia is seen as a fundamentally critical infrastructure where the security of telecommunications networks has become of vital importance for the functioning of the society. Hence, it can be stated that the proposal most probably has legal ground to outweigh the infringement of the freedom of enterprise. However, the aim or the reason behind the discrimination must be fairly balanced against the disadvantage caused because of the discrimination. This means it must be appropriate and necessary.  

It should be taken into account that if there are better and less discriminatory ways of doing the assessment according to the proposed draft, it would be more difficult to justify discrimination.

As the Board of National Defense and The Armed Forces stated on a law proposition in France, damage resulting from malicious acts would be very heavy to deal with *ex post* and, if the control rules were to be tightened later, the companies would have to bear costly corrective investments. Moreover, *ex ante* assessment approach seems ultimately more reassuring for detecting the vulnerabilities. It was also said to be inevitable that such a procedure of investigation may require some time and cause some inconvenience. However, the importance of ensuring the resilience of telecommunications networks justifies the assessment procedures. In any event, the key to the fluidity of the procedure lies in anticipating requests - it is recommended for companies to initiate discussions for *ex ante* assessments on their projects already in their early stage, prior to entering the market.

Even so, the limits of authority are important enough to impede enforcing the presented proposal. The regulation is constitutional only if it is in compliance with the limits, idea and aim of authority. The Ministry of Justice has found that technical requirements for communications networks and requirements for the provision of communications services when necessary for reasons of public policy or public security are procedural requirements that must be provided on the level of law.

---


31 Ibid.

The solution to this issue would be to submit a thorough analysis that would indicate why the infringement of the freedom of enterprise according to section 31 of the Estonian Constitution is justified with the current regulation, taken into account that the proposal stands for compelling state interest.33

2) The Ministry of Justice finds that the proposal is not in accordance with the constitution. According to subsection 17 (4) of the General Part of the Economic Activities Code Act such secondary requirements for permits can only be added in the cases and extent provided for by law34 and the Ministry of Justice does not find that the grounds provided in subsection 87 (1) and clause 87 (2) 4) of the Electronic Communications Act are sufficient, as they do not concern requirements procedural requirements.35

The solution to this issue would be to amend the Electronic Communications Act in such a way that it would provide a legitimate basis for the regulation and the procedural requirements.

This could be done by amending subsection 87 (2) of the Electronic Communications Act in the following way:

“2) Based on the principles and objectives provided for in subsection 1 of this section, the Government of the Republic may establish technical requirements for the communications networks and requirements for the provision of communications services as well as procedural requirements for granting the permit to provide communications services, if this is necessary for: ”.

This would be a broad addition that first allows for the specific procedural requirements as proposed in the current amendment but also would allow for other procedural requirements to be added if it is necessary for national security. This gives the state a greater freedom for the future, as it is not easy to predict how the technology will change and whether this will add more risks that might have to be mitigated through different requirements.

3) The Ministry of Justice has found that the wording of section 3\(^1\) to be flawed. The wording indicates that it is only necessary to provide the technical information, rather than to get cooperation and approval from the Consumer Protection and Technical Regulation authority.\(^{36}\) In order to remove the ambiguity of section 3\(^1\), it should be reworded such that it is made clear that the secondary requirement is not merely submitting the technical information but actually getting approval from the Consumer Protection and Technical Regulation authority.

With this in mind, the authors propose that subsection 3\(^1\) (5) be amended in the following way:

“Consumer Protection and Technical Regulation Authority makes **getting the approval laid out in** from subsection 1 a **secondary requirement for getting frequency authorisation.**”

In this case, it would be emphasized that it is not only the act of submitting the technical information for approval but rather getting the approval itself that is a secondary requirement for communications undertakings.

4) It is not entirely clear what kind of information must be provided and if it must be done once for the whole network topology as a whole or for each piece of equipment, including in case one piece of equipment is changed, will it need to be resubmitted for approval. Finally, the section speaks about giving technical information but does not provide any other checks whether or not the company is in fact going to use the equipment submitted for approval.\(^{37}\)

Here, it must be taken into consideration that there has to be a balance between obligations put on the service provider and interests of national security. On the one hand, with regards to national security, it is good to get as much information as possible, so that it is easier to exclude companies that might have malicious intent. On the other hand, there is the question of what is reasonable to expect from the other party and whether asking information about every single component might put an undue burden on the communications undertakings. Furthermore, this would also put a burden on the authorities, who have to evaluate the applications of the communications undertakings.

---

\(^{36}\) *Ibid.*

In addition, while the information required to be provided with the technical documentation, would be something the communications undertakings would presumably have to possess anyway, as they should be aware, what kind of hardware and software and for what purpose they are using, there is also the question of volume of information. It seems providing the information for each individual component would not be that difficult, however, considering the complexity of network infrastructures, the sheer volume of information to be provided and in turn analyzed by authorities might be too burdensome. Such infrastructure can contain a very large number of software and hardware components and it is probably unreasonable and unnecessary to evaluate every single piece of wire or other component. Therefore, a distinction should be made between components that require evaluation and those that might require less scrutiny.

Taking that into consideration, the authors recommend subsection 3\(^1\) (1) should be amended in the following way:

“.../Technical documentation of the hardware and software of the communications network must include at least the following for each network infrastructure master/active/primary device:.../”

According to the authors' opinion, asking technical documentation of each network infrastructure device might be too burdensome and even impossible. Therefore, the authors find that a distinction should be made between different types of components, to lessen the burden on both the communications undertaking and the regulatory authority. One option is to distinguish components based on the “master” and “slave” distinction, where master devices\(^{38}\) are devices that can guide the data exchange in the network and slave devices\(^{39}\) are devices that receive and reply to data sent by master devices\(^{40}\). Previously mentioned terms could also be replaced with different terms like “active”/“passive” and “primary”/ “secondary”, depending on the exact definition the authorities deem the best.

However, it requires sector-specific in-depth knowledge to determine whether this is the best way to separate components based on the risk they embody. Therefore, further

---

38 In Estonian “ülemseade”.
39 In Estonian “alamseade”.
analysis is required by experts with more knowledge of the technical side of such networks and their topology.

In addition, the authors would add the following subsection to section 3\(^1\):

“(1) The Consumer Protection and Technical Regulatory Authority may require the communications undertaking to present additional documentation to be provided for other hardware and software components, if they deem it necessary.”

This amendment would give the opportunity to request information on other components as well, because it is possible that some potentially dangerous components might not fall under the amended section 3\(^1\). It might not be possible to differentiate fully between components that require extra scrutiny and those that do not. Therefore, it is important to give the Consumer Protection and Technical Regulatory Authority the opportunity to widen the scope of the components of which they ask technical documentation, as they see necessary if they have additional security concerns.

5) The Ministry of Justice has brought out a terminological inconsistency as the current Administrative Procedure Act defines approval (in Estonian “koostöö”) as something one administrative body gives another during the course of administrative procedure. This, however, is not administrative procedure but authorization procedure. Approval would be granted by the security authorities.\(^{41}\)

Taking all this into consideration, subsection 3\(^1\) (1) could be reworded in the following way:

“Communications undertaking named in subsection 87 (4) of the Electronic Communications Act will provide for approval to the Consumer Protection and Technical Regulation Authority technical documentation of the hardware and software of the communications network before starting to use the hardware and software of the communications network. Technical documentation of the hardware and software of the communications network must include at least the following: /.../”

Here in the Estonian version the word “kooskõlastamine”, which is used in administrative procedure and already has a different meaning, is substituted with “heakskiit” to avoid confusion. “Heakskiit” or in English “approval” indicates that the

\(^{41}\) Ibid.
information will be submitted to the authority and they in turn will decide if the technical documentation for the proposed communications network is sufficient with regards to national security. Based on that, they will either approve it (in Estonian “kiidavad heaks”) or leave it unapproved (“jätavad heaksikiidu andmata”).

6) Finally, while it falls outside the scope of this work, the Ministry of Justice has also indicated that the regulations should involve ways to check equipment already in use.\textsuperscript{42} This might be done by adding provisions into the law that provides the Consumer Protection and Technical Regulation with the right to conduct inspections to ensure the equipment used does not constitute a threat to national security, either before it is taken into use or even after. There is also a question of what to do when a company substitutes individual pieces of equipment after getting the initial approval\textsuperscript{43}. This could be solved by requiring that communications undertakings submit technical documentation for approval when they need to replace an approved component for another.

\textsuperscript{42} Ibid.  
\textsuperscript{43} Ibid.
3. Legal solution

3.1. Solutions from Other Member States

While the EU Member States retain sole competence for matters of national security as mentioned above, and the EU’s role is complementary, the Member States have taken different approaches to mitigate security threats.

For example, Germany's Federal Network Agency has set complementary security requirements for telecommunication networks and services in its “security catalogue”, i.e. the use of critical key components being made subject to certification. Moreover, security requirements apply to all network operators and service providers, irrespective of the technology they deploy. However, concerns are related to the German “security catalogue” regarding a “no-spy decree” that would be required to sign by the telecom operators when identifying critical parts of their networks. That would technically obligate a telecom provider only to make a promise to have trustworthy suppliers of critical components. Taking into account the risks at stake, the given legal approach should be avoided, especially regarding the core parts of the network that handle critical information. It is also questionable whether the security requirements are necessary to be applied to all network operators and service providers, irrespective of the technology they deploy.

French government on the other hand, has taken new legal provisions in 2019 in regards fifth generation and subsequent generations of mobile radio networks, requiring full government access to suppliers’ technology. Legal solutions can be seen upon Chapter II of title I of book II of the Post and Electronic Communications Code Section 7 “Prior authorization scheme for the operation of radio network equipment”. This has set out which equipment is subject to authorization in order to preserve the interests of defense and national security, naming all material devices or software on the national territory of devices that may present a threat. The authorization is required for the operation, directly or through third-party suppliers of devices.

---

by the operators. The authorization to operate a device may be granted after examining an authorization request file submitted by the operator.\textsuperscript{49} It may be refused to grant the authorization if it is considered that there is a serious risk of harm to the interests of defense and national security.\textsuperscript{50} Moreover, amongst many other conditions for the assessment of this risk, it is taken into consideration that the operator or its service providers, including by subcontracting, is under the control or subject to acts of interference from a state which is not a member of the European Union.\textsuperscript{51} Furthermore, if the operation of the devices is carried out on the national territory without prior authorization or without respecting the conditions fixed by the authorization, the operator may be ordered to file an authorization or renewal request or to have the previous situation restored at his expense.\textsuperscript{52} These injunctions mentioned above however, can only intervene after the operator has been given formal notice to present observations within fifteen days, except in the event of emergency, exceptional circumstances or imminent threat to national security.\textsuperscript{53}

Italy has taken a straight-forward approach and amended its legislation to allow the government to block contracts with non-EU telecoms providers.\textsuperscript{54} According to the amendments to the decree-law 15 March 2012, No. 21, and 11 May 2012, No. 56 regarding defense and national security, the external parties of the European Union are defined. Secondly, it is stipulated that contracts/agreements should be provided concerning the purchase of critical components or services related to the components of outside the European Union. They can be subject to the notification for the purpose of any exercise of veto power or the imposition of specific requirements or conditions. Furthermore, the components that are already implemented and that could compromise the integrity and security of the networks and data passing through, are also subject to evaluation of vulnerability factors.

As seen from a few examples above, the Member States do not have a unified legal approach towards telecommunications providers of the EU and third-country companies. The solution depends on a state how explicitly it would choose to differentiate the EU companies and third-country companies considering the threats. In any event, it would be advised to have appropriate security measures on all counterparts in a prior authorization regime to regulate access to the

\textsuperscript{49} LOI n° 2019-810 du 1er août 2019 art. L. 34-11.-II.
\textsuperscript{50} LOI n° 2019-810 du 1er août 2019 art. L. 34-12.
\textsuperscript{51} LOI n° 2019-810 du 1er août 2019 art. L. 34-12.
\textsuperscript{52} LOI n° 2019-810 du 1er août 2019 art L. 34-13.-I.
\textsuperscript{53} LOI n° 2019-810 du 1er août 2019 art. L. 34-13.-I.
telecommunications market for reasons of national security. France, has set a great example for other Member States, including Estonia, how an *ex-ante* assessment could be implemented, whereas Italy has shown that veto power to block contracts with non-EU telecoms providers is legally feasible.

**3.2. Amendments to the Electronic Communications Act**

The objective of the amendments made is to have only reliable technology used in the Estonian telecommunications market. Companies shall not be separated into different categories. Market access will be regulated on the grounds of risk assessment, considering the risk profile of the companies.

All the proposals regarding the amendments of the Electronic Communications Act as well as the draft regulation of the Government of the Republic shall be done having the Rules for Good Legislative Practice and Legislative Drafting taken into account. All of the amendments below are meant to be used together with the amendments already made above in the second chapter.

**3.2.1. The Power to Establish a Verification Procedure**

Our first recommendation would be to supplement section 87 of the Electronic Communications Act in such a way as to provide basis for verification procedure. The authors believe this is necessary to ensure that in case where technical documentation seems to be in order, but there is still doubt that the company might be submitting technical documentation not in accordance with the actual equipment used by the communications provider. In such a situation a government agency should have the competence to do inspections of the hardware and software before (and possibly after) they are taken into use.

Even though, sections 133 and 133¹ of the Electronic Communications Act already regulate state supervision more generally, this would give the government the opportunity to add extra measures not outlined in the Law Enforcement Act, that may be specific to evaluating communications networks.

---

Based on this, the authors propose the following as subsection 2\textsuperscript{1} to section 87:

“(2\textsuperscript{1}) Based on the principles objectives provided for in subsection 1 of this section, the Government of the Republic and may establish a procedure to \textit{inspect} whether an undertaking adheres to the requirements laid out for the communications networks and the provision of communications services, if this is necessary for:

1) ensuring national security.”

An authorising provision grants the right to establish a regulation of the Government of the Republic to inspect whether an undertaking adheres to the requirements laid out for the communications networks and the provision of communications services. In this case, the verification procedure can be done at the level of the Regulation. For example, all telecommunications networks are reliant on software controlled equipment\textsuperscript{56} and this amendment gives authorities the right to implement procedures to have access to potential suppliers’ technology, e.g. access to telecommunications software, including encryption keys and code which does not come from the current law.

3.2.2. Amendments to the Regulation of June 22, 2016 No. 140 “Requirements for provision of communications services and technical requirements for communications networks”

The authors of this work find that the recent amendments to the regulation “Requirements for provision of communications services and technical requirements for communications networks” contain some appropriate methods to assess the security aspects of the company's hardware and software components. Therefore, the authors also use the ideas and wordings of the amendments made. However, in some places, the authors found that there was a need to change the wording and add few additional security measures.

Based on this, the authors of this work support the idea that subsection 1\textsuperscript{1} to section 3 should be added:

“(1\textsuperscript{1}) it would be in accordance with national security interests”

The authors define the concept of “national security” in the same way as the working group of the draft. The goal of Estonian security policy is to retain Estonia’s independence and

sovereignty, territorial integrity, constitutional order and public safety.\textsuperscript{57} According to the Ministry of Defence national defense is described as a collection of broad-based activities, including the continuity of operation of vital services.\textsuperscript{58} Service providers pursuant to Electronic Communications Act subsection 87 (4), whose services are consumed by at least 10,000 end-users, shall be providers of the vital services in respect of the phone, mobile phone and data transmission services. Therefore, the communications undertakings providing vital services consumed by no less than 10,000 end-users, may have an impact on national security.

The authors also propose the following as subsections 1, 2 and 3 to section 3:\textsuperscript{1}

“Section 3\textsuperscript{1} subsection 1 Communications undertaking named in subsection 87 (4) of the Electronic Communications Act will electronically provide for approval to the Consumer Protection and Technical Regulation Authority technical documentation of the hardware and software of the communication network before starting to use or before replacement the hardware and software of the communications network. Technical documentation of the hardware and software of the communications network must include at least the following for each network infrastructure master/active/primary component:”

This requirement only applies to the provider of a vital service who is according to the Electronic Communications Act subsection 87 (4) a telephone, mobile and data service provider with at least 10 000 end-users. Such a solution should ensure that authorities have information of what sort of components vital service providers use in their networks.

The change to “master/active/primary component”\textsuperscript{59} has been outlined already in chapter 2 subsection 2.2 point 4.

The change to “for approval”\textsuperscript{60} has been outlined already in chapter 2 subsection 2.2 point 5.

The amendment “or before replacement” has been added because currently the regulation states that software and hardware must be submitted for approval before it is taken into use\textsuperscript{61}. This, however, in our opinion leaves it unclear whether this is required every time a new hardware or software component is added to the network infrastructure or only when entering the market.

The addition would clarify that this approval is required every time a component is replaced

\textsuperscript{57} Julgeolekupoliitika. The Estonian Ministry of Foreign Affairs. Online: https://vm.ee/et/taxonomy/term/49 (04.01.2020).


\textsuperscript{59} In Estonian ülemseade, aktiivseade, esmane seade.

\textsuperscript{60} In Estonian change from “kooskõlastamine” to: “heakskiit”.

\textsuperscript{61} Nõuded sideteenuse osutamisele ja sidevõrkude tehnilised nõuded. § 3\textsuperscript{1} lg 1.
with another. While this does not strictly deal with the core issue of how to keep malicious companies away, the authors believe that it could have preventative value. To be more precise, it would show the companies who want to enter the market with malicious intent, that they cannot just start off with technology that is approved and then after getting approval change it out with different technology. Knowing that all changes require re-submission for approval, should act as a deterrent as they would know they cannot just get past the first approval and then start using different equipment.

1) the name of hardware and software;”

This requirement provides an opportunity to evaluate more easily hardware and software security.

“2) name of the company who has produced the hardware and software;”

This requirement helps to ensure that the communication networks are set up and communication services are provided by a reliable company. Moreover, it gives the opportunity to assess whether the company is an European company or a third-country company and also whether there are any specific concerns over security relating to that particular company. For example, if a company providing hardware or software is in majority owned by a state, that could indicate a potential red flag. To illustrate, according to the report of the EU coordinated risk assessment of the cybersecurity of 5G networks, third-country suppliers corporate governance presents notable differences, e.g. in terms of level of transparency and type of corporate ownership structure.

Furthermore, several Member States have identified that certain third-country companies represent a particular cyber threat to their national interests, based on previous modus operandi of attacks by certain entities or on the existence of an offensive cyber programme of a given third country against them. In addition, the individual risk profile of suppliers will become particularly important, especially where a supplier has a significant presence within networks or areas. Therefore, it is important to assess the risk profile of the technology manufacturer and to avoid the influence of unreliable suppliers.

“3) the function of hardware and software in the communications network;”

---


63 Ibid.
Authorities need to know the purpose of the network infrastructure components because it enables assessing the components’ security aspects. This way it is clear why the component is necessary, so components with malicious or unclear purpose cannot be added. In addition, depending on what the function of the component is, the requirements regarding security might be different - a core component would presumably have to adhere to stricter standards of security than some less vital components, which, when attacked, would be a lesser vulnerability.

“4) the place of use of hardware and software in the communications network;”

Authorities need to know how and where the components are used in practice. This requirement is needed because some geographic areas might be particularly sensitive, e.g. some areas might suffer greater disruption due to the economic and societal reliance on network and information systems or because sensitive entities or users are located in them. Therefore, components in certain areas can require particular attention and this requirement facilitates assessing the components’ security aspects.

“5) the beginning and end date of the use of hardware and software.”

The authors believe this is a necessary requirement as it helps to provide a general overview of how long time a network infrastructure component will be in use. This also helps as the authors have added the requirement to section 3 subsection 1 that each piece of equipment that needs to be replaced be submitted to approval. Knowing when a component would need to be replaced and the communications would need to ask for approval again, would help the state with having an overview of whether the communications undertaking is adhering to the regulation.

The explanatory note of the proposed draft argued that the state has a responsibility to ensure that communications networks are built on reliable technology, the use of which would not lead to a situation in which the state could not guarantee the protection of the fundamental rights and freedoms for its citizens, including privacy, message confidentiality and intellectual property. Therefore, inspection of the technical documentation of the hardware and software ensures that the company uses secure network components.

“(2) The Consumer Protection and Technical Regulatory Authority submits information set out in section 3 subsection 1 clauses 1-5 to the security authorities and to the Information System Authority. These authorities shall, within 30 working days of being consulted, give their opinion

64 Ibid.
as to whether the putting into service of the communications network hardware and software is in the interest of national security. The Consumer Protection and Technical Regulatory Authority may extend the deadline by a maximum of 30 days. To extend the deadline, the Consumer Protection and Technical Regulatory Authority will have to provide the communications undertaking with written reasoning for the extension as well as the new deadline.”

The reason for this is because the authors doubt that 30 days is enough to give a comprehensive opinion. This is also in connection with the fact that the authors are of the opinion that the technical documentation should be given about every component of the network. This means it could potentially be quite a large amount of information to analyze. Therefore, to ensure that the analysis does not suffer due to lack of time and that the Consumer Protection and Technical Regulatory Authority can make a thorough assessment, the authors have added the addendum that this 30 day deadline can be extended if necessary for an additional 30 days. However, in order to ensure that the communications undertaking does not have to wait unnecessarily, the decision to extend the deadline must be provided in writing along with both reasoning on why it was necessary and a fixed new deadline to make sure that the Consumer Protection and Technical Regulatory Authority may only take more time if it is necessary and it is strictly regulated.

In addition, The Consumer Protection and Technical Regulatory Authority submits technical documentation to other authorities because it has not cyber security assessment competence.66

“(3) The Consumer Protection and Technical Regulatory Authority in making a decision referred to in subsection 4 may, if necessary, request a reasoned proposal from the Cyber Security Council of the Security Committee of the Government. Mentioned Council shall submit a reasoned proposal to the Consumer Protection and Technical Regulatory Authority within 60 working days of the date of the request.”

The authors are of the opinion that 60 days gives the Council enough time to deliver its reasoned proposal while not burdening the other party unduly either, and thus, the authors did not make any changes to this subsection.

---

66 Ibid.
“(4) The Consumer Protection and Technical Regulatory Authority decides whether to give the approval within 30 working days of the date of receipt of the opinion referred to in subsection 2 or the date of receipt of the proposal referred to in subsection 3.”

The change here is “on the approval”. The reasoning is explained in chapter 2 subsection 2.2 point 5. The Consumer Protection and Technical Regulatory Authority has to decide whether or not it approves the technical documentation of the telecommunications company's communications network hardware and software within 30 working days of the date of receipt of the opinion or proposal. This should guarantee that the company can put into operation the communications network hardware and software only after The Consumer Protection and Technical Regulatory Authority has given their approval.

“(5) The Consumer Protection and Technical Regulatory Authority makes getting the approval laid out in subsection 1 a secondary requirement for getting frequency authorisation.”

The change here is “the approval arising”. The reasoning is explained in chapter 2. The explanatory note of the proposed draft stated that this subsection establishes a mechanism for the suspension of the frequency authorization granted to a telecommunications undertaking which is in breach of the obligations set out in subsection 3\(^1\) (1) of the draft and, if the infringement continues, to be revoked.\(^{67}\)

Since the work analyzes telephone, mobile and data service providers who provide vital services then legal solution should also ensure that the interruption of these services would be minimized so as not to pose a threat to the life or health of people or to the operation of another vital service. Therefore, national law should enable that in case of emergency or exceptional circumstances, telecommunications company could replace a component immediately without prior authorization. However, authorities should still get the information of what sort of components the provider uses in its networks to be able to evaluate the threat the company might pose to national security and thus, the company should be required to submit the technical documentation later.

Based on this, the authors of this work propose the following as subsection to be added to section 3\(^1\):

“(6) In case of exceptional circumstances, if there is a risk of disruption of vital services, the communications undertaking may without prior authorization replace components in the

\(^{67}\) Ibid.
network infrastructure. The communications undertaking is then required to within 14 working days after replacing a component, to submit technical documentation to the Consumer Protection and Technical Regulatory Authority. If the component is not approved by the authority, then the communications undertaking is required to replace the component.”

Last but not least, the authors also recommend considering the following measures:

In our opinion, it may be beneficial to include into the required technical documentation the information about where the hardware and software has been manufactured. This could be applied primarily to master/active/primary components, to provide an extra layer of assurance of trustworthiness, in case the question of threat to national security stems less from the telecommunications undertaking and more from its subcontractors.

The question remains whether asking technical documentation of the components of the communications network is too burdensome for the communications undertaking. Even if the requirement is not for every single component, it could still mean a lot of information that the communications undertaking has to provide. To lessen the burden and make getting the approval an easier process, the Consumer Protection and Technical Regulatory Authority might provide the communications undertakings with forms to fill out with the requested technical information. That way if it is clear and easy for the communications undertaking to provide the requested information and they do not have to do unnecessary extra work. Similarly, this will make it easier for Consumer Protection and Technical Regulatory Authority to check the provided technical documentation as it will all be provided in a unified manner.

Previously mentioned issues should also be taken into consideration, as although they do not relate to the entering the telecommunications market, they are important from the standpoint of national security. These measures should help to prevent that some other components are used and ensure that the hardware and software documented are actually put into service.

It is important to recognise that some threats to the telecommunications network are global or external in character, so national legislation alone cannot solve everything and thus, there is also a need to develop regulations at the level of the European Union to counter issues related to national security of Member States.

SUMMARY

The objective of this work is to offer a legal solution of how Estonia could prohibit a company entering its telecommunications market when consisting a threat to its national security. The solution is achieved by focusing on the recent amendment proposals made on the 15.11.2019 to the regulation of June 22, 2016 No. 140 “Requirements for provision of communications services and technical requirements for communications networks,” the explanatory note of the regulation, the rejection of 23.12.2019 by the Ministry of Justice and the Electronic Communications Act.

The given work sets forth that Member States of the EU can implement prior authorization regime to regulate access to their telecommunications market for reasons of national security. Member States can also choose whether to differentiate the EU companies and third-country companies considering the threats, as the telecommunications companies are subject to Member State’s national law. Nevertheless, in this work the same measure has been implemented for both EU companies and third-country companies.

Considering the importance of the topic and the amount of work already done on the national level by the expert group and the Ministry of Economic Affairs and Communications, this work concentrates on how the amendment proposals could be improved with the Electronic Communications Act in a way to have a legal ground for an ex ante risk assessment and subsequently, a legal ground for regulating market access considering national security in Estonia.

Taken into account the main purpose of the proposed draft - creating telecommunications market conditions to ensure public order and national security - the discrimination of section 31 of the Estonian Constitution is found to be justified. In the view of the objective, the proposal has a legitimate aim that is outweighing the infringement of the freedom of enterprise. Moreover, Estonia would not be a pioneer in the EU by implementing such prior authorization regime.

It has been noted that the current Electronic Communications Act needs to be changed in such a way to provide a legitimate basis for the regulation and the procedural requirements. Thus, the paper suggests amending the wording of Electronic Communications Act subsection 87 (2) and doing it so that it would also apply to the future technologies. Additionally, the paper suggests rewording sections of the proposal in order to remove the issues with ambiguity and
terminological inconsistency by making the requirements clear to the communications undertaking.

Moreover, the work offers supplementary proposals on how to regulate access to the telecommunications market for reasons of national security. It is advised supplementing section 87 of the Electronic Communications Act in order to provide basis for verification procedure for a government agency to have the competence to do inspections of the hardware and software before (and possibly after) they are taken into use. The work adds suggestions for amending the “Requirements for provision of communications services and technical requirements for communications networks” to emphasize the national security interests and gives an opinion on the sections already drafted.

Furthermore, specific subsections are advised to the regulation for further requirements regarding the technical documentation as well as some changes to deadlines to give the Consumer Protection and Technical Regulatory Authority enough time to analyze the technical documentation. The paper finds also necessary to further emphasize in law that each master/active/primary component that needs to be replaced should be submitted for approval and the section does not concern only companies first entering the market.

In addition, a section was added to ensure that in case a vital service is in danger, fixing the infrastructure will not be delayed by waiting for approval. In this case, if sufficient reason is provided, the component can be submitted for approval after it has been installed.

And lastly, considering the critical sectors dependent on information and communication technologies, it would be strongly advised to implement security checks as a preventive measure in order to keep telecommunications companies that impose a threat to national security from entering with the intention to start off with technology that is approved and then after getting approval replace it with different technology.
BIBLIOGRAPHY

Legal acts and policy documents


**Literature**


APPENDIX 1

The translations for all the proposed changes in law and regulation.

Changes in the Electronic Communications Act

Section 87 subsection 2

(2) Vabariigi Valitsus võib, lähtudes käseseleva paragrahvi lõikes 1 sätestatud põhimõtetest ja eesmärkidest, kehtestada sidevõrkude tehnilised nõuded ja nõuded sideteenuse osutamisele ja kehtestada proseduurilisi nõudeid sideteenuste osutamiseks loa andmisele, kui see on vajalik:

Section 87 subsection 2¹

Vabariigi Valitsus võib, lähtudes käseseleva paragrahvi lõikes 1 sätestatud põhimõtetest ja eesmärkidest, kehtestada proseduurilisi nõudeid, millega kontrollida, kas sideettevõtja järgib sidevõrkudele ja sideteenuste osutamisele kehtestatud nõudeid, kui see on vajalik:

1) avaliku korra ja riigi julgeoleku tagamiseks.

Changes in the regulation “Requirements for provision of communications services and technical requirements for communications networks”

Section 3 subsection 1¹

see oleks kooskõlas riigi julgeoleku huvidega

Section 3¹ subsection 1

Elektroonilise side seaduse § 87 lõikes 4 nimetatud sideettevõtja esitab elektrooniselt Tarbijakaitse ja Tehnilise Järelevalve Ametile heakskiidu saamiseks sidevõrgu riist- ja tarkvara tehnilise dokumentatsiooni iga sidevõrgu ülemseadme/aktiivseadme/esmase seadme kohta enne sidevõrgu riist- ja tarkvara kasutusele võtmist või välja vahetamist.

Section 3¹ subsection 1¹

Tarbijakaitse ja Tehnilise Järelevalve Amet võib kohustada sideettevõtja esitama täiendavat tehnilist dokumentatsiooni ülejäänud tarkvara ja riistvara kohta, kui nad peavad seda vajalikuks.

Section 3¹ subsection 2

Tarbijakaitse ja Tehnilise Järelevalve Amet esitab lõike 1 punktides 1–5 toodud teabe julgeolekuasutustele ja Riigi Infosüsteemi Ametile. Nimetatud asutused annavad oma
arvamuse, kas sidevõrgu riist- ja tarkvara kasutuselevõtmine vastab riigi julgeoleku huidule, 30 tööpäeva jooksul arvamuse küsimisest arvates. Tarbijakaitse ja Tehnilise Järelevalve Amet võib arvamuse andmise tähtaega pikendada veel kuni 30 päeva. Tähtaja pikendamiseks peab Tarbijakaitse ja Tehnilise Järelevalve Amet esitama sideettevõtjale kirjaliku põhjenduse koos uue tähtajaga.

**Section 3**

**subsection 3**

Vajaduse korral küsib Tarbijakaitse ja Tehnilise Järelevalve Amet lõikes 4 nimetatud otsuse tegemisel Vabariigi Valitsuse Julgeolekukomisjoni Küüberjulgeoleku Nõukogu põhjendatud ettepanekut. Nimetatud nõukogu esitab Tarbijakaitse ja Tehnilise Järelevalve Ametile põhjendatud ettepaneku 60 tööpäeva jooksul ettepaneku küsimisest arvates.

**Section 3**

**subsection 4**

Tarbijakaitse ja Tehnilise Järelevalve Amet otsustab heakskiidu andmise 30 tööpäeva jooksul lõikes 2 nimetatud arvamuse või lõikes 3 nimetatud ettepaneku saamise päevast.

**Section 3**

**subsection 5**

Tarbijakaitse ja Tehnilise Järelevalve Amet seab lõikes 1 nimetatud heakskiidu saamise kohustuse sagedusloa kõrvaltingimuseks.

**Section 3**

**subsection 6**

Erakorraliste asjaolude esinemisel, et vältida törkeid elutähta teenuse pakkumisel võib sideettevõtja ilma eelnevat heakskiitu saamata komponente välja vahetada. Sellisel juhul peab sideettevõtja 14 tööpäeva jooksul pärast komponendi asendamist esitama Tarbijakaitse ja Tehnilise Järelevalve Ametile komponendi kohta käiva tehnilise dokumentatsiooni. Kui komponent ei saa heakskiitu, peab sideettevõtja selle välja vahetama.