TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Liis Peedu

IMPLEMENTATION OF NETWORK AND INFORMATION SYSTEMS SECURITY DIRECTIVE 2016/1148 IN REPUBLIC OF ESTONIA: BALANCING TRANSPARENCY AND SECRECY

Master's thesis

Programme in Law, specialization Law and Technology

Supervisor: Agnes Kasper, PhD

TALLINN 2018

I declare that the I have compiled the paper independently

and all works, important standpoints and data by other authors

have been properly referenced and the same paper

has not been previously been presented for grading.

The document length is 19145 words from the introduction to the end of conclusion.

Liis Peedu ……

(signature, date)

Student code: 162912HAJM

Student e-mail address: liis.peedu@gmail.com

Supervisor: Agnes Kasper, PhD:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defense Committee:

Permitted to the defense

……

(name, signature, date)

Contents

ASO – data communication network for public authorities

CERT – computer emergency response team

CSIRT – computer security incident response team

DNS – domain name systems

EISA – Estonian Information System Authority

ENISA – European Union Agency for Network and Information Security

GDPR – General Data Protection Regulation

HÕNTE – Rules for Good Legislative Practice and Legislative Drafting

ICT – information communication technology

ISKE – information systems security system

IXPs – Internet exchange points

MS – Member State(s)

NATO – the North Atlantic Treaty Organization

NIS Directive – Network and Information Systems Security Directive

TLD – top-name domain registry

X-road – data exchange layer

ABSTRACT

In recent times the European Union legislators have proposed and adopted multiple regulatory instruments, which help to ensure high cybersecurity level throughout the Union. From these legislative initiatives or in force regulatory instruments, it is clear that the European Union wants to move towards better information sharing and collaboration between Member States and to enhance the public-private cooperation to better the security of cyber domain.

In 2013 the European Union Commission proposed the NIS Directive. The NIS Directive preamble alludes that differences between Member States within network and information security regulations would impede the trade between Member States and would even become an obstacle on sustaining and further developing the internal market. Based on this argumentation it was found that the best results would be achieved with the Union level legislation.

Estonia, as a Member State of the European Union must transpose all Union legislative measures. NIS Directive is no different.

This dissertation will answer following research questions:

What are the legal obstacles that prevent the application of transparency norms in relation to NIS implementation in Estonia?

Does the implementing law strike fair balance between secrecy and transparency?

Estonia has established itself as a true e-government state. Most of the Estonians use the Internet to conduct their businesses and to communicate with the government and its institutions. Everyone owning an ID-card can get access to their medical history at any time, night or day. This connectivity has had its benefits, but at the same token it has brought up a lot of debates over the security of these systems and how much dependency on the Internet is really safe to have.

In Estonia, all legislative processes begin with so called background research of established laws and whether these in force laws have scope, which is required to regulate whichever field necessary at that time. This strategic question helps to come to a unified understanding whether a new law is necessary or could Estonia, or any state, rely on existing legislation. Relying on in force legislations is also described in law literature as the evolutionary approach.

The principles of transparency and secrecy must be balanced. Only if those two principals are balanced can there be as optimal regulation as possible. Without any transparency there would be no control and partnership between private and public parties. On the other hand, same could be told about secrecy, without any secrecy there could be no effective defensive legislation nor, again, trust between parties because some secrecy principles must be ensured.

Keywords: secrecy, transparency, NIS Directive, Republic of Estonia, legislative process, cybersecurity, information security, implementation of the Union law

1. INTRODUCTION

In this dissertation the reader will be given a comprehensive overview of the network and information systems security directive (hereinafter also NIS Directive), which is one of the newest pieces of legislation within the field of cybersecurity. The reader shall be introduced to the main points and ideas of the NIS Directive, while discussing their necessity for securing the European Union cybersecurity.

This thesis shall view the implementation of NIS Directive in Estonia. The reader will be given an overview of the legislative process in Estonia. Additionally, the reader will be introduced to Estonian national online instruments which help to ensure transparency, while at the same time make Estonia vulnerable to cybersecurity breaches.

Additionally, in master's thesis the reader shall be given an overview of cybersecurity related developments within the European Union and what have been the main issues thus far in securing cyberspace.

The main research issue of this thesis is the transposition and implementation of the NIS Directive in the Republic of Estonia. The core issues assessed in this thesis are transparency and secrecy, and balancing the two seemingly conflicting principals in cybersecurity legislation.

The thesis will over provide a quick overlook of what transparency and secrecy mean in cybersecurity – thus far there are many opposing views on this question. While some see complete transparency as a way of honesty, it is not always a wise choice, others see secrecy as being inseparable part of the core of cybersecurity.

Master thesis will follow the implementation process in Estonia and discusses the possible problems and obstacles on the road to new or improved legislation(s). Many different positions on implementation of NIS Directive exist, while some want to draft completely new law, others

see it more reasonable to update existing laws – master thesis will give an overview of both sides and their positive and negative implications.

The reader will be given an overview of new draft legislation and its main weak points in balancing of transparency and secrecy. The new draft legislation, which is the Estonian Parliament for 2nd reading, has had many supporters but more opposing entities. Entities have seen little effort to make the new legislation private entity friendly while respecting their rights, for example, for business secrets. Moreover, many have seen the new legislation as a way of government agency getting increasing access and power over private entities' data, which has raised questions about network and information systems security and log data which they produce.

The research questions, which this master's thesis will try to answer are following:

What are the legal obstacles that prevent the application of transparency norms in relation to NIS implementation in Estonia?

Does the implementing law strike fair balance between secrecy and transparency?

While the dissertation aims to answer two main research questions, this work will also introduce the reader to other questions and problems which may raise when trying to implement European Union legislation or when trying to regulate cybersecurity related matters.

In order to fulfill the aim of the master's thesis research and to answer the two main research questions, text analysis methodology was chosen. The reader will be presented with argumentation which is based on legal texts, legislations, academic articles and other important sources which include relevant information on the topic. The before mentioned sources add to the depth of the argumentation as well as give this dissertation a sense of legal analysis.

2. OVERVIEW AND BACNKGROUND OF NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2016/1148

2.1. Cybersecurity in the European Union

The European Union (hereinafter also the Union) ancestor European Coal and Steel Community was built, after the World War II, to be more of a preventive measure against a highly possible World War III. Later the Union started developing, slowly but surely, into a more coherent union of the states, which aimed to develop a single market and common defense mechanisms.

Since the late '90s the Union has continuously worked towards strengthening the ability to act autonomously as a military force.[1] The European Union has made really impressive progress in its Foreign and Security Policy throughout the inception of the Union. Not only has the Union worked hard on its autonomous military capabilities, it has worked toward transnational military cooperation.

The European Union has established multifaceted economic, diplomatic and military means to fight against the physical threats. The Union has close ties with NATO, and has established well working military cooperation with the United States which thus far has been without great hiccups.

While the Union has made substantial efforts to assure the protection against physical, more of a traditional war, it has long jogged behind many nations when it comes to network and information systems security, or overall cybersecurity. But being in the 21st century and seeing the ever growing cyber-security threats which may become issues of national or even international security threat, it is imperative to act. Thus far, the European Union has been taken more of a passive role in promoting cybersecurity related issues.[2]

[1] Posen, B. R. (2006). European Union Security and Defence Policy: Response to Unipolarity? – *Security Studies,* Vol. 15, No. 2, 149-186, p. 178.
[2] Sliwinski, K. R. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent. – *Contemporary Security Policy,* Vol. 35, No. 3, 468-486, p. 468-469.

Additionally, even though the European Union Member States (hereinafter also referred to as MS) see, for the most part, eye-to-eye when it comes to the physical security of nations, it tends to be far different scenario when talking about cybersecurity. These differences could stem from the fact that the European Union is not a federacy where there is a central government, rather it is a union of states, which have individually and freely decided to be a part of a union of states. The European Union relies heavily on the intergovernmental cooperation, while MS' sovereignty has outmost respect.

This difference, where there are local national governments and no truly central governmental institutions has led the European Union to a state where all or most MS have defined cybersecurity and cyber threats as their nation sees it. Thus far there has been no collective vision on what exactly cybersecurity entails.[3] Without the common language and clarity on the core definitions of cyber domain it is no wonder that the European Union has struggled to be seen as a leader in cybersecurity or even compatible partner internationally. Moreover, true cooperation also demands high-quality decision making in national laws and also true transparency within these regulations.[4]

This passiveness from the European Union together with no clear notion on what exactly cybersecurity is, has led the whole Union and its MS to a state where the exposure to cybersecurity threats are elevated. Not only is there a lack of mutual understanding, there is a lack of harmonization between Member States' cybersecurity strategies.[5]

Additionally, even though the European Union has promoted cooperation between Member States in different areas, it has not truly elevated the collaboration in cybersecurity domain. True cooperation can only come when the Union MS are obliged explicitly by Community law[6]

[3] *Supra nota.*, p. 469.
[4] Wenander, H. (2013). A Network of Social Security Bodies – European Administrative Cooperation under Regulation (EC) No 883/2004. – *Review of European Administrative Law,* Vol. 16, No. 1, 39-71, p. 62-63.
[5] Sliwinski, K. F. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent. – *Contemporary Security Policy,* Vol. 35, No. 3, 468-486, p. 470-472.
[6] Lafarge, F. (2010). Administrative Cooperation between Member States and Implementation of EU law.- *European Public Law,* Vol. 16, No. 4, 597-618, p. 598-603.

and directed to share information amongst nations, private entities and of course the citizens and residents.

In recent times the Union legislators have proposed and adopted multiple regulatory instruments, which aim to secure cyber sphere and which contain breach notification requirements.[7] From these legislative initiatives or in force regulatory instruments, it is clear that the European Union wants to move towards better information sharing and collaboration between Member States and to enhance the public-private cooperation to better the security of cyber domain.

2.2. New legislative efforts towards cybersecurity

The passive attitude of the European Union legislators came to a halt in 2013. In early February of 2013, which was later renewed in 2017[8], the European Commission released a joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.[9]

The released cybersecurity strategy's one of the key messages was the crucial need for the European Union wide strategy to undertake the ever growing cybersecurity related challenges. Moreover, to promote and secure fundamental rights and freedoms in cyber domain, like the European Union has done in the physical world.

[7] Esays, S. Y. (2014). Breach Notification Requirements Under The European Union Legal Framework: Convergence, Conflicts, and Complexity In Compliance. – *The John Marshall Journal of Information Technology & Privacy Law,* Vol. 31, Issue 3, Article 2, 317-368.
[8] European Commission Joint Communication to the European Parliament, the Council JOIN(2017) 450 final 13.9.2017 Resilience, Deterrence and Defense: Building strong cybersecurity for the EU.
[9] European Commission Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions JOIN(2013) 1 final of 7.2.2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure cyberspace.

To strengthen individuals' rights and freedoms on the cyber domain, the European Union legislators released General Data Protection Regulation (hereinafter also GDPR) (2016/679)[10] in 2016. The before mentioned European Union regulation ensures high rights of individuals, while introducing higher level of technical and organizational security measures for data controllers and processors.

Additionally, the GDPR imposes a data breach notification obligation to data controllers. While data controllers are obliged to notify Supervisory Authority, data processors have the duty to notify data controller. Moreover, it is important to note that the GDPR imposes an obligation to data controller to notify directly natural persons, whose personal data has been an object of a breach, when there is a likelihood of persons affected to come under the direct violation of their rights and freedoms. This multilevel breach notification duty aims to better accountability of data controller and processors.

Together the GDPR and the NIS Directive, the European Union legislators have shown more and more initiative to promote security in cyber domain. In addition, both the GDPR and the NIS Directive can be considered one of the cornerstones of Digital Single Market strategy.[11]

The European Union for extended period of time as seen national security as a part of an overall Union wide security, where the true key to success comes from cooperation. Even though physical security has been seen a Union wide matter, cybersecurity in most part has been viewed more of a national security issue,[12] which should be tackled individually by each state.

[10] The European Parliament and the Council of the European Union (EU) No 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 04.04.2016.
[11] Webber, M., Taylor, S. (2016). The NIS Directive – a practical perspective. – *Privacy & Data Protection,* Vol. 16, Issue 3, 9-12, p. 11.
[12] e Silva, K. (2013). Europe's fragmented approach towards cyber security. – *Journal on internet regulation. Internet Policy Review,* Vol. 2, Issue, 4, 1-8, p. 2-3.

One of the key vision points of cybersecurity strategy[13] was to achieve and ensure cyber resilience of the whole European Union. Cyber resilience could be considered one of the cornerstones of cybersecurity, because resilience means the ability to bounce back from errors and attacks with non to minimal damage. A resilient network or information systems is far more reliable than weak network and information systems, it seems obvious. In the case of making the networks and information systems more resilient, it is not to be forgotten that the European Union, MSs and private sector must also work towards reliability of these. Reliable performance of networks and information systems is essential also.[14]

Additionally, resilient and reliable networks and information systems must endure different types of errors.[15] This means that whatever attacks may be aimed to bring down an essential service provider operators, they must be able to endure such attacks and not only to endure but also be able to continuously provide their services without or with minimal disruptions.

Unfortunately, the European Union cybersecurity strategy[16] still lacks the definition of cybersecurity. This again, could mean continuously fragmented approach to cybersecurity amongst the European Union MSs. Again, cybersecurity definition has not explicitly given in the Union cybersecurity strategy, but one could find a definition to this on the webpage of the European Union Agency for Network and Information Security (abbreviated to ENISA). On the webpage of ENISA, cybersecurity has been defined as follows: ‘’Cybersecurity covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. /…/, cybersecurity should cover the following attributes:

[13]Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions JOIN(2013) 1 final of 7.2.2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure cyberspace.

[14] Denyer, D., Kutsch, E., Lee-Kelley, E., Hall, M. (2011). Exploring reliability in information systems programmes. – *International Journal of Project Management,* Vol. 29, 442-454, p. 443-444.

[15] Kreutz, D., Malichevskyy, O., Feitosa, E., Cunha, H., da Roda Righi, R., de Macedo, D. D.J. (2016). A cyber-resilient architecture for critical security services. – *Journal of Network and Computer Applications,* Vol. 63, 173-189, p. 180.

[16] European Commission Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions JOIN(2013) 1 final of 7.2.2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure cyberspace

Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability /…/ Robustness, Survivability, Resilience /…/, Accountability, Authenticity and Non-repudiation /…/.''[17]

In order to achieve this visioned cyber resilience, cooperation is needed amongst different level players within the Union. True resilience can only be accomplished by strong collaboration and cooperation between all Union MSs, public and private bodies.

It is important to note that the European Union's acknowledgement of the importance of public-private cooperation is meaningful or even momentous. This acknowledgement is essential due to the reality that most of today's cyber domain is owned by private sector rather than public. Consequently, mostly private sector owned cyber world cannot achieve resilience without the joint efforts of public and private sectors.

Across the Union there are MSs which have successfully introduced and incorporated public-private collaboration into their cybersecurity legislations. Additionally, quite a few MSs have introduced voluntary commitments. But this uneven legislation level has left a very fragmented approach across the Union.

2.3. Network and Information Systems Security Directive proposal

The NIS Directive[18] aims to establish high common level of security of networks and information systems across the European Union.

The proposal recommended all Union MSs to firstly name national competent authorities, secondly to set up a well-functioning computer emergency response team (also abbreviated to

[17] ENISA. ENISA overview of cybersecurity and related terminology. Version 1, September 2017. Accessible: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology. Last accessed on: 02.02.2018.

[18] The European Parliament and the Council of the European Union (EU) No 2016/1148 of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union, OJ L 194/1, 19.07.2016.

CERT), thirdly to adopt national network and information system security strategy and a national cooperation and collaboration plan on network and information systems security.

Moreover, the proposal[19] for NIS Directive made a proposition to set up coordinated prevention, detection, mitigation and response mechanism. This mechanism was aimed to enable international information sharing and mutual assistance when coming under network and information system attack or incident.

Further, the NIS Directive proposal was also intended to better and deepen the private sectors engagement and readiness when dealing with cybersecurity. This engagement would not only benefit private sector but also public sector and of course the citizens of the European Union.

At a time where cybersecurity threats embark havoc across the world, the NIS Directive aims to tackle the risks which are imposed in the cyber domain cyber domain.[20] The NIS Directive has an ambitious objective to increase the cybersecurity readiness, resilience of networks and information systems. Mostly NIS Directive is aimed to secure critical networks and information systems in paramount sectors of society and economy.

Thus far, private sector has been reluctant to adopt and embrace good risk management culture. NIS Directive aims to establish a highly dependable cooperation between public and private sector, where the security obligation is shared between the two actors.

In addition, private sector can see cybersecurity as measure which is with high cost and no one really knows what this security would entail. This makes the whole cyber domain less secure across the Union. The lack of regulations thus far has made it hard to communicate cybersecurity issues between private sector and governments, and this in return has made

[19]European Commission Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions JOIN(2013) 1 final of 7.2.2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure cyberspace

[20] Holzleitner, M.-T., Reichl, J. (2017). European provisions for cyber security in smart grid – an overview of the NIS-directive. – *Elektrotechnik & Informationstechnik,* Vol. 134, No. 1, 14-18, p. 14.

cybersecurity information sharing between Member States' governments and institutions close to non-existent.

The proposed NIS Directive aims to better information sharing and convince the reluctance of private sector to collaborate with governments. One of the objectives of NIS Directive proposal was to encourage private entities on specified sectors to embrace cybersecurity risk assessments. This in return would be a great way to make private entities to realize which security risks they faced and would result in risk mediation measures. Moreover, public sector would benefit from such risk management culture as well. Public sector would be able to collect and process information provided by private sector. This information would enable to assess the overall national cybersecurity level.

Additionally, not only would national competent authorities be able to collect and receive data about security risk assessments, these authorities would be notified of significant cyber incidents which have occurred in the networks or information systems of essential service providers or critical infrastructures.

The proposal foresaw that national competent authorities should exchange information about cyber incidents, especially in cases where there had been involvement of personal data. Moreover, the proposal obliged the national competent authorities to inform law enforcement authorities, in case of incidents where serious criminal activity had been suspected. These serious criminal activities could range from possible money laundering to suspected espionage.

Withal, the European Union Commission also stressed that for the development of single market, it is significant to look at network and information systems security less as a burden and more as a way to enhance Europe's competitive advantage.[21]

[21] European Commission Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions JOIN(2013) 1 final of 7.2.2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure cyberspace.

After the release of the Union's cybersecurity strategy and the companying Network and Information Systems Security Directive, the Parliament and the Council of the European Union took it to deliberations. Both the Parliament and the Council assured the importance of such legislation on the Union level.

2.4. Adoption of NIS Directive and an overview

The European Union's Internal Security Strategy[22] took an aim to fight against most critical and demanding security issues. In the Internal Security Strategy, the Union has listed the most urgent threats such as terrorism, cyber-crime, organized grime, the management of the Unions external borders and last but not least civil disasters. The European Union Internal Security Strategy was released in 2010, even at that time cyber-crime was seen as immediate threat which could materialize.

Even though it has been acknowledged that the Union needs a common approach to cyber security, the European Union's cyber security strategy has also been criticized for not truly bringing MSs together to secure the cyber domain. For example, Dutch member of the European Parliament, Sophie Veld, has denounced the strategy for lacking true strategic measures and for having little initiative to actually unify the fragmented cybersecurity issues amongst the Member States.[23]

Before the proposal of NIS Directive, the Union legislators had tried, with little success to regulate cyber domain. Some of the initiatives include the proposal for a Networks and Information Policy, multiple programs and policies on critical infrastructures. Policies, which created no legally binding duties on the operators of these critical infrastructures.[24] After the

[22] European Commission Communication to the European Parliament, the Coucil COM(2010) 673 final of 22.11.2010 The EU Internal Security Startegy in Action: Five steps towards a more secure Europe.
[23] Baker, J. (2013). *Top politician slams EU cybersecurity plans.* Accessible: https://www.networkworld.com/article/2163018/security/top-politician-slams-eu-cybersecurity-plans.html. Last accessed: 03.02.2018.
[24] Fahey, E. (2014). The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security. – *European Journal of Risk Regulation,* Vol. 5, Issue 1, 46-60, p. 49-51.

unsuccessful use of soft law methods, the Union legislators set its aims at more constructed regulation methods.

It is important to note that the European Commission does not completely back down from the soft law methods, as the strategy does involve awareness raising exercises, transatlantic cooperation, and so on.

After some failed attempts to achieve cyber domain security, the European Union Commission proposed the NIS Directive. The NIS Directive preamble alludes that differences between Member States within network and information security regulations would impede the trade between MSs and would even become an obstacle on sustaining and further development of internal market.[25] Based on this argumentation it was found that the best results would be achieved with the Union level legislation.

Without the common direction by MSs, cyber security field has come to a place where there are very different approaches to cyber security. The Union, as an ecosystem of states, would much more benefit from common and cooperative approach. Additionally, due to the fact that cyberspace in its essence is trans-border and transnational domain, it is only appropriate that effective cybersecurity calls for trans-border and transnational cooperation[26] between MSs and 3rd countries.

The European Union's critical infrastructures and essential services are more and more intertwined. Additionally, the European Union is working towards cyber single market. Cyber single market would mean that equality as it is in physical market of goods would apply also to the cyber domain market places. This would mean that in some years Internet stores could not pick and choose where they send their goods, rather all Member States' citizens and residence could enjoy equal market. These changes would further deepen the interrelations between

[25] *Supra nota.* p. 51-55.
[26] Sliwinski, K. F. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent. – *Contemporary Security Policy,* Vol. 35, Issue 3, 468-486, p. 476-478.

Member States. For these aspirations to become a reality, a harmonized approach to cybersecurity is imperative.

Networks and information systems have grown to be the very backbone of the European Union and its Member States economy. Growing number of different systems are online, more and more goods can be bought online, not to mention that our critical infrastructures are online. These developments have led the Union to realizing that these systems must be secure and breach information must be shared in order to be more resilient and ready to counteraction.

2.5. Objectives and reasoning for the NIS Directive

The objectives and reasoning for NIS Directive is the fact that the European Union as a whole is growingly more dependent on information systems and networks. These networks and information systems could come across security incidents such as malicious attacks or simple human error. It is obvious that lack of sufficient network and information systems security could bring down essential services, this in return would also negatively affect the European Union's economy and welfare of people.

Additionally, growing number of services and goods can be facilitated via Internet using information systems. These services in return can plays an important role in free movement of services, goods and people – the functioning of internal market. If big disruptions are taking place in one MS, these could affect and have adverse effect in other MSs. Considering the interconnectedness of the European Union's MSs and their networks and information systems it is clear that for the better functioning of internal market, it is imperative to have resilient and stable networks and information systems.

Additionally to low success rates of voluntary approaches to cybersecurity, there has also been uneven distribution of competence amongst MSs and also vastly different levels of readiness in case of network and information systems incidents.[27] The contrasting differences between the

[27] e Silva, K. (2013). Europe's fragmented approach towards cyber security. – *Journal on internet regulation. Internet Policy Review,* Vol. 2, Issue 4, 1-8, p. 4-7.

Union's MSs, leaves the co-dependent networks and information systems vulnerable and leaves little room to build trust amongst Member States to share necessary cybersecurity information.

2.6. Legal basis

The legal basis for the NIS Directive is compiled in Article 114 of the Treaty on the Functioning of the European Union. Since network and information system security play a great part in the functioning of the internal market operations it is in the scope of legislative power of the Union's legislators.

Before the NIS Directive, the Union's legislators have acknowledged the growing need to harmonize network and information systems security. With the Regulation on establishing the European Network and Information Security Agency,[28] the Union legislators made it clear that network and information systems security must be harmonized in order to ensure the functioning of internal market.

In addition, when talking about the legal elements of the NIS Directive, it is important to note the principle of subsidiarity, which was first mentioned in Article 5 of the Treaty on European Union. In its core, the subsidiarity principle aims to protect the Union MSs from overreaching Community powers by limiting legislative powers to what is strictly necessary at times where Member States are unable to achieve goals by individually regulating.[29]

In regards to regulating network and information systems, it is clear that harmonized security standards would be best achieved on the European Union level rather than individual regulations by each Member States. Since network and information systems across the Union are so intertwined and are a huge part of internal market it is clear that it is wiser to drift away from only national legislations to supra-national regulations.

[28] The European Parliament and the Council (EU) No 460/2004 of 10 March 2004 establishing the European network and Information Security Agency, OJ C 220, 16.09.2003, p. 33.
[29] Timmermans, C. (1998). Subsidiarity and Transparency. – *Fordham International Law Review,* Vol. 22, Issue 6, Article 8, 106-126, p. 106.

Additionally, it is important to mention the principle of proportionality. The Union legislators chose minimum harmonization measures to regulate network and information system security. This means that MSs are still free to adopt measures which would be suitable for their nation taking into account risks it may face. In regards to the NIS Directive, it sets out minimum standards which must be followed by Member States. This minimum harmonization promotes more harmonious network and information system security as well as cooperation between Member States and also between private and public sectors.

To conclude the legal aspects of the NIS Directive proposal, it is clear that best network and information system security can only be achieved on the Union level. This is due to the nature of networks and information systems being borderless, meaning that incident in one Member State could have an effect in other Member State(s). In compliance with principles of subsidiarity and proportionality it clear that the European Union legislator may adopt measures in the scope of network and information systems security.

To enforce the NIS Directive, ordinary legislative procedure started. Ordinary legislative procedure is a legislative process in which the Council and the Parliament act collaboratively to adopt and mend legislative proposals.[30] The legal basis for such legislative procedure comes from the Treaty on the Functioning of the European Union, Article 294.

2.7. Approval of NIS Directive and fundamental pillars

In December of 2015, the European Parliament, the Council and the Commission finally reached an agreement on the text of NIS Directive.[31] After the political agreement was reached in 2015[32], the European Parliament adopted the NIS Directive in July of 2016 and the Directive

[30] Craig, P., de Burca, G. (2015). *EU Law: Text, Cases, and Materials.* 6th edition. 1-1159, p. 126-133 Oxford University Press.
[31] The European Parliament and the Council of the European Union (EU) No 2016/1148 of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union, OJ L 194/1, 19.07.2016.
[32] Burden, K. (2015). European Union Update. – *Computer Secuirty & Law,* Vol. 31, 810-815, p. 815.

entered into force in August 2016. Member States had 21-month-period to implement the NIS Directive.

The NIS Directive embodies three fundamental pillars:

1. ensuring Member States preparedness by requiring to assemble Computer Security Incident Response Team (in short CSIRT) and national competent network and information security authority

2. ensuring cooperation between Member States by assembling a Cooperation Group (to ensure cooperation and swift information exchange amongst Member States) and a CSIRT Network (to ensure effective operational cooperation and information exchange in time of cybersecurity incidents and possible risks)

3. ensuring a culture of cybersecurity across vital sectors of economy and society. These vital sectors of economy include businesses active in energy, water, banking, transport, financial market infrastructures, healthcare and digital infrastructure, additionally key digital service providers such as cloud computing services, online marketplaces or search engines. These sectors are now obliged to adhere to the security and breach notification requirements under NIS Directive.

It is appropriate to note that similar requirements already apply[33] to telecom operators and internet service providers under the ePrivacy Directive 2002/58. It is also appropriate to note that the Union legislators are working towards new the ePrivarcy Regulation.[34]

[33] Esayas, S. (2014). Breach Notification requirements Under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance. – *The John Marshall Journal of Information Technology & Privacy Law,* Vol. 31, Issue 3, Article 2, 317-368, p. 329-334

[34] European Commission. Proposal for a Regulation on Privacy and Electronic Communications COM(2017) 10 final of 10.1.2017. Accessible: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications. Accessed: 13.02.2018.

2.8. Overview and aims of the NIS Directive

The objective of the NIS Directive is to achieve and ensure a high common level of security of network and information systems across the European Union Member States. Common level of security would be accomplished by improving national level and the Union level cooperation and by promoting safe information sharing amongst Member States.

Additionally, the NIS Directive aims not only to promote cooperation between nations but also between private entities and governments. To achieve such cooperation, the operators of essential services and digital service providers shall be required to mitigate their security risks. Moreover, the essential services operators and digital service providers shall be required to report security breaches to national competent authorities.

Further, the NIS Directive also aims to require MSs to adopt national strategies concerning cybersecurity. The national cybersecurity strategies should combat the issues which will ensure high levels of network and information systems security within the scope of essential services. Additionally, the NIS Directive Chapter II, Article 7 sets out the particular issues which national strategies need to address.

Additionally, the NIS Directive also sets out the prerequisite of reporting national strategies to the Commission within three months of adopting cybersecurity strategies. While cybersecurity strategy must be reported to the Commission, the Member States may exclude strategy points which would expose the overall national security measures.

To achieve objectives set out by the proposal, the European Union cybersecurity strategy, and by the NIS Directive the Member States must assemble multiple national cybersecurity focused authorities.

Additionally to competent authorities and single points of contact, the Member States must also designate at least one national Computer Security Incident Response Team (also CSIRT). Every

Member State's national CSIRT shall also be a part of a European Union wide CSIRT network. The aim of establishing CSIRT network is undoubtedly to promote trust between Member States and to ensure a well-functioning information exchange ecosystem. Unfortunately, the NIS Directive gives almost no procedural rules for CSIRT network, therefore it is up to the network to decide how tasks will be officiated.

In addition to all actors' groups which must be established by the MSs, the NIS Directive also call for a Cooperation Group to be established on the Union level. The Cooperation group shall be composed of representatives of each Member State, ENISA, and of the Commission.

Cooperation Group provision was not included in the Commission's 2013 proposal for the NIS Directive. Rather the proposal foresaw Cooperation network, was to be consisted of national competent authorities and the Commission.[35] After the European Parliament's first reading, some changes were made to the members of Cooperation Group. In the proposal for the NIS Directive the Commission had suggested that national competent authorities would be a part of the Cooperation network, while the Parliament had strongly suggested that the single points of contact should be involved to have more stable information change within the Group.

Coming to a national level of the Network and Information System Security Directive, it is a duty of each Member States to identify operators of essential services. The NIS Directive itself gives guidance on the criterions[36] which should be taken into the consideration. It is also important to note that the NIS Directive imposes an obligation on European Union Member States to oversee the list of essential service providers every two years and this updated list if needed.[37] It is indisputable that a supervision over this kind of obligation is necessary, therefor

[35] European Commission Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union COM(2013) 48 final of 7.2.2013. Accessible: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013PC0058. Accessed: 8.05.2018

[36] The European Parliament and the Council of the European Union (EU) No 2016/1148 of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union, OJ L 194/1, Article 5, point 2.

[37] Burden, K. (2016). European Union Update. – *Computer Law & Security Review,* Vol. 32, 363-368, p. 364.

the NIS Directive sets out the supervisory duty of the essential services operators list to the Cooperation Group.

In the Commissions 2013 proposal for the NIS Directive, the Commission foresaw the need to include the public administrators as obligated actor to ensure appropriate technical and organizational measures to ensure the security of networks and information systems. Additionally, public administrators were seen to have a notification duty of breaches. The European Union Parliament did not agree with the Commission's proposal on that and removed the public administrators off the list. In the adopted NIS Directive, the only obliged persons are operators of essential services and digital service providers.

Even though both essential service providers and digital service providers are obliged under similar duties, the enforcement and implementation of these duties somewhat differ from one another.[38] For instance, the essential service operators can be a subject to an audit, more specifically to a security audit. The essential service operators audit shall be conducted by competent national authority.[39] While digital service providers are not a subject to a security audit, rather they are under the requirement to provide information regarding implemented technological and organizational security measures.

The urgency and the importance of securing networks and information systems is caused by the fact that growing number of information systems are interconnected. This co-dependency can lead to a situation where one company is facing security risk, all entities in connection with the first could become a liability.

The interconnected business partners could together be exposed to network-wide risks, which are not just limited to a single risk.[40] These risks could include a simple computer system virus,

[38] *Supra nota.*
[39] The European Parliament and the Council of the European Union (EU) No 2016/1148 of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union, OJ L 194/1, Article 15, point 2.
[40] Fang, F., Parameswaran, M., Zhao, X., Whinston, A.B. (2014). An economic mechanism to manage operational security risks for inter-organizational information systems. – *Information Systems Frontiers,* Vol. 16, Issue 3, 399-416, p. 400-402.

becoming a victim to malicious hacking, coming under denial-of-service attacks, and so on. Based on multiple risks and their possible outcomes, it seems evident that securing these interconnected information systems and networks should be the European Union's goal especially at a time where systems and networks are becoming more co-dependent on the Union level.

The NIS Directive is divided into seven chapters. Firstly, the NIS Directive starts with the first chapter, the General Provisions. This chapter of the NIS Directive introduces the aims of the Directive and also the obligations of MSs when implementing the NIS Directive. Additionally, the first chapter also introduces the reader to the scope of the NIS Directive.

In addition, Article 2 of the NIS Directive indicates which legislations shall be applicable when processing personal data. Even though the NIS Directive was adopted in 2016, so should be fairly up-to-date it does not have an indication to the GDPR. Instead the NIS Directive still implies to the old Union legislation, the Directive 95/46/EC[41] which was overturned by the GDPR. Unfortunately, there is no reference to the new data protection regulation.

Additionally, Article 3 of the NIS Directive sets out the aim of minimum harmonization amongst the European Union Member States. The European Union MSs have very fragmented approach to cybersecurity so the NIS Directive aims to establish harmonized minimum standards for purpose of internal market and of course for the development of digital single market.

Further, Article 4 of the NIS Directive might be one of the Articles which has most importance. Article 4 of the Directive gives important definitions for the MSs to apply. These definitions shall serve as a gateway to more understanding between Member States when applying NIS Directive rules and when coming under network or information systems attacks.

[41] The European Parliament and the Council (EU) No 95/46/EC of 24 of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31.

Additionally, NIS Directive Article 4 sets out unified standard and understanding of what exactly are security incidents and risks when talking about network and information systems, and so on. It is a positive step towards bringing the MSs closer together when tackling cybersecurity incidents in networks and information systems.

Furthermore, the first chapter of the NIS Directive consists of Article 5. Article 5 has great importance when Member States are working towards implementation of the Directive. Article 5 sets out the directions to the MSs on how to identify the essential services operators.

The last Article of the chapter one of the NIS Directive is Article 6.[42] Undoubtedly, Article 6 is also with great significance, since it sets out the principles of determining whether an incident in network or information systems has significant effect. Determining significant disruptive effect is essential due to the fact that, based on this analysis the Member States' agencies can decide if information sharing and cooperation measures are necessary. It is especially important when essential service operator is the only operator on specific market field and whether the operator provides services across the European Union.

Article 7 of the NIS Directive sets out the obligation to compile a national strategy on security of network and information systems security. In addition to setting up such an obligation, the NIS Directive also provides guidance for minimum standards for such national strategies. Moreover, Article 7 sets out the duty to report national strategies to the Commission. The reported national strategies can be free from overall national security elements. This exclusion is welcomed because national security is the highest priority point of each Member States and making available such information to employees who might not be bound by secrecy nor confidentiality, may pose a great security risks for all Member States.

Further, as mentioned beforehand, MSs are required to set up national competent authorities, single points of contact and computer security incident response team. These requirement stems

[42]The European Parliament and the Council of the European Union (EU) No 2016/1148 of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union, OJ L 194/1, Article 6.

from Articles 8; 9; and 10 of the NIS Directive.[43] From the European Union legislator it is wise to ask the Member States to have necessary agencies which are equipped with necessary organizational and technical measures to provide support, smooth communication channels, and all around support on a national and supra-national level. These measures could bring many Member States which do not have at this time such agencies more up to speed with Member States that have such teams. This, again, would even out the differences between cybersecurity levels between the Member States.

Chapter three of the NIS Directive focuses on the cooperation between the Union and Member States, and cooperation between the European Union and third countries outside the Union. Additionally, chapter three of the Directive also establishes a CSIRT network, which is aimed to also build trust between MSs and to ensure quick and adequate operational cooperation.

It is clear from chapter three of the NIS Directive that the European Union legislators have aimed to provide the Member States with cooperation agencies which they could trust to work together with mutual ambition to secure network and information systems security.

Chapter four of the NIS Directive provides the Member States' national legislators with the security requirements of the network and information systems for essential services operators. Additionally, the fourth chapter's Articles also provide incident notification requirements for operators of essential services.

Moreover, in accordance with the NIS Directive, the operators of essential services must dully notify national competent authority or national CSIRT of incidents with significant effect. Member States are obliged to ensure that necessary steps are taken to impose such notification obligation.

[43] *Supra nota.,* Article 8-10.

In addition, the NIS Directive Article 14, point 4 lists parameters which are useful when assessing whether an incident may have significant effect.

These parameters include:

'' /…/

a) the number of users affected by the disruption of the essential service;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident.''[44]

It must be noted that these parameters allow quite a wide interpretation. There are no set-in-stone quantities tied with these parameters, so each essential services operator must make their own assessments in that regard. This may result in uneven reporting and insufficient collaboration between the private sector and national governments and its institutions.

Additionally, if operators are free to interpret these parameters, national agencies may not get sufficient and needed information which they ought to share with other Member States. This in return might result in lack of trust and sense of information closure.

As with many security breach notification legislations in the European Union, the NIS Directive imposes fines, if not complied with the obligations.[45] These fines can be seen as a very forceful way to make operators comply, but if a network and information systems security is the ambition, these disciplinary actions must be taken.

[44] The European Parliament and the Council of the European Union (EU) No 2016/1148 of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union, OJ L 194/1, Article 14, point 4, a-c.
[45] Laube, S., Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. – *Journal of Cybersecurity,* Vol. 2, Issue 1, 29-41, p. 29-31.

Moreover, the NIS Directive Article 15[46] ensures that national competent authorities remain in a position to ensure the compliance with the imposed obligations to operators of essential services. To corroborate the compliance with the obligations, the national competent authorities are allowed to request information which is deemed necessary to assess security of network and information systems. Additionally, competent authority must be provided with sufficient evidence to, in essence, prove effective implementation and enforcement of security documents such as intra-group security policy.

These enforcement methods can raise multiple confidentiality issues. Since the NIS Directive does not imply directly that these documents are to be kept secure and in a confident manner, many operators may be reluctant to share obliged information in a fear of giving out potentially compromising information.

Additionally, the Article 15 of NIS Directive imposes a duty on competent authorities to provide operators with the purpose and specification on information requested. Unfortunately, the Directive does not provide circumstances on which an essential service operator could refuse to give out information nor does the Directive imply to any time frame in which the operator should comply with such requests.

Similarly, to chapter four of NIS Directive, chapter five introduces security requirements and incident notification obligations of digital service providers. Firstly, it is appropriate to note that digital service providers under the NIS Directive are:

1. online market places;

2. online search engines; and

3. cloud computing services.[47]

[46] The European Parliament and the Council of the European Union (EU) No 2016/1148 of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union, OJ L 194/1, Article 15

[47] *Supra nota.*, Annex III

So according to Annex III of NIS Directive, digital service providers are everyone from Microsoft Azure cloud system to auto24.ee. It is a quite wide range of service providers, which in addition, also need to comply with the GDPR[48] notification obligation as well. This can potentially confuse the service providers at a time of security breach, since a question is raised whether they would need to notify multiple authorities or just pick between two possibilities. Additionally, double notification obligation could impose also a monetary burden for entities, which need to gather sufficient information and send notifications to multiple authorities which would all result in time lost to focus on their everyday business.

Likewise, with operators of essential service, digital service providers must also notify national competent authority and national CSIRT of incidents which may have substantial effect on provided service. In addition, digital service providers must also include in their notifications any and all information on significance of cross-border impact.

In contrast to operators of essential services, digital service providers must only notify of incidents where the provider has access to necessary information to evaluate the impact of a security incident against the notification parameters. These parameters are following:

’’/…/

(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident;

(d) the extent of the disruption of the functioning of the service;

(e) the extent of the impact on economic and societal activities.’’[49]

[48] The European Parliament and the Council of the European Union (EU) No 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 04.04.2016.

[49] The European Parliament and the Council of the European Union (EU) No 2016/1148 of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union, OJ L 194/1, Article 16, point 4, a-e

To enforce the duties of NIS Directive to digital service providers, the Member States must warrant national competent authorities with the right to take action when necessary with supervisory measures. It is important to note that such measures can only be evoked when national competent authority has been provided with evidence which shows, that digital service provider is not in compliance with its obligations under the NIS Directive.

The supervisory measures can be conducted through requesting necessary information from digital service providers. This information could include either description of technical and organizational measures taken for security and any and all security policies implemented in an entity. Additionally, national competent authority may require the digital service providers to remedy any and all unsatisfactory fulfillment of obligations under the NIS Directive Article 16.[50]

With digital service providers it is clear that some or even most of them could be providers outside the Union, this in return raises an issue of applicable jurisdiction. Article 18 of NIS Directive[51] deals with the issue of jurisdiction. Accordingly, digital service providers shall be a subject to whichever Member State's jurisdiction in which it has its main establishment. And according to the Article 18, the location of main establishment shall be in correlation with the location of service providers headquarter. While digital service providers which are established outside of the European Union are obliged to name a representative within the Union. These digital service providers which have named representative, must offer their services within this MS where the representative is named.

Additionally to mandatory security breach notification obligations, the NIS Directive chapter six introduces voluntary notification measures.[52] Under this chapter any and all entities which are not named as operators of essential services nor digital service providers may voluntarily notify national authorities of security incidents which may have significant effect on the continuity of any services these entities provide. While the Directive provides that voluntary notifications shall be secondary to mandatory breach notifications, meaning that mandatory

[50] *Supra nota.*, Article 16.
[51] *Ibid.* Article 18
[52] *Ibid.* Articles 19-20

notifications shall be processed beforehand. Moreover, voluntary breach notifications may be completely left unprocessed if excessive burden is brought on by these notifications.

In the view of network and information systems security it seems unnecessary to promote voluntary breach notification opportunity if no use is made of information provided on voluntary bases. Under the NIS Directive, micro- and small digital service providers are excluded from the notification obligation. This cause potentially excludes many enterprises, which could be intertwined with each other and due to connection is network or information systems could still result in significant disruptive effect.

3. TRANSPOSITION AND IMPLEMENTATION OF NIS DIRECTIVE IN REPUBLIC OF ESTONIA

3.1. E-Estonia and e-services importance

Estonia has established itself as a true e-government state. e-Government can be defined as using the Internet to deliver information about government and number of services to its citizens via World Wide Web.[53] Many, if not most, of Estonians use the Internet to conduct their businesses and to communicate with the government and its institutions. Everyone owning an ID-card can get access to their medical history at any time, night or day. This connectivity has had its benefits, but at the same token it has brought up a lot of debates over the security of these systems and how much dependency on the Internet is really safe to have.

Regardless of security issues, Estonia with its government and people has been promoting itself as a true digital forerunner and an e-government state. To some extent it could be considered true, especially since many foreigners tend to look towards Estonia when implementing e-government solutions. Most of Estonia's success has come due to the fact that Estonia has made ID-card mandatory for all citizens.[54]

Estonia has made it possible to use a single ID-card, which is issued by the Police and Border Guard Board, for essentially all services provided by the government and even private sector. Additionally, Estonia has been the first European Union Member State (even the first nation overall) to open its digital borders to non-citizens.[55]

The fact that Estonia does indeed issue ID-cards for foreigners, shows the true interest of Estonia to appeal to international businesses and attract more investments. This again, plays together with the Digital Single Market strategy. Based on the before mentioned factor, we

[53] Hwang, K., Choi, M. (2017). Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism. – *Government Information Quarterly,* Vol. 34, 183-198, p. 184.
[54] Isikut tõendavate dokumentide seadus, §5, section 1. RT I 1999, 25, 365
[55] Sullivan, C., Burger, E. (2017). E-residency and blockchain. – *Computer Law & Secuirty Review,* Vol. 33, 470-481, p. 470.

could say that Estonia has tried well to establish well-functioning digital ecosystem for Digital Single Market agenda.

Due to the fact that Estonia is so invested in all things ´e´, meaning many, if not most of our essential services are available online, interactive and interconnected, it seems quite evident that it is in Estonia's best interest to have outstanding network and information systems security policy and strategy.

Virtually all people in Estonia are the owners of ID-cards, therefore all information systems attached and available should be able to withstand and be resilient to cybersecurity scares. Moreover, since ID-cards are issued to non-citizens, the responsibility to ensure network and information systems security widens to these third country ID-card owners equally.

In addition, it is significant to mention that Estonia has promoted e-voting. This means that all citizens owning a ID-card could vote without physically going to a voting station. All a person would need is their ID-card and correct PIN codes, which are only known by the owner of the card. This system must be secure enough so it would withstand any tampering so honest results could be drawn. The author sees ID-card and its opportunities as critical infrastructure in the Estonian cyber world.

Again, when it comes to critical infrastructures, essential services and so on, governments should be seen as the responsible actor for the safety. Governments are in position to impose rules and regulations on private sector players who provide essential services, therefore the obligation to ensure the security of such networks and information systems should lay with the governments.

Moreover, even though critical infrastructures, essential services and such are owned by private sectors, the governments still have jurisdiction over national security and private sector owned services which are online may become a national security risk. Most of essential services are connected to networks and multiple information systems, which make them vulnerable to

cybersecurity threats. These threats pose a real life danger to the functioning of democratic society – this becomes a national security issue. Therefore it is reasonable to conclude that the governments duty to protect its citizens, indeed extends to the cyber domain.[56]

3.2. Network and information systems' dependence in Estonia

In 2007 Estonia and its population saw what a cybersecurity breach could cause to its nation. The mere fact that Estonian government had made a decision to move the Red Army era memorial to more fit place caused Estonia to become a target of large scale cyber-attacks. These cyber-attacks left a clear message to the world that cyber domain could be used to undermine the functioning of any nation and its citizens. Estonia's attacks, which were most likely conducted by Russia and its governments marionettes, left Estonia's largest bank essentially paralyzed and many of the credit card companies were forced to take down their systems.[57] So most of the cyber-attack targets were privately owned entities, which conducted their businesses under the Estonian jurisdiction – this shows that it must be every governments' best interest to secure these networks and systems so that the sustainability of normally functioning society would be possible.

In addition, as of 2017 Estonia roads have been introduced to electronic traffic and road signs.[58] Whichever network and information systems these traffic and road signs are connected to, need to be as secure as possible. Due to the nature of these signs, a malicious actor could display information which could lead to hazardous situations.

Based on the before written examples, it is extremely important to secure these critical and essential networks and information systems. It is virtually impossible to avoid cyber-attacks,

[56] Shore, J. J. M. (2015). An Obligation to Act: Holding Government Accaountable for Critical Infrastructure Cyber Security. – *International Journal of Intelligence and CounterIntelligence,* Vol. 28, Issue 2, 236-251, p. 238.
[57] Sales, N. A. (2013). Regulating Cyber Security. – *Northwestern University Law Review,* Vol. 107, No. 4, 1503-1568, p.1505-1507.
[58] Kahu, O. (2017). Pärnu maanteele tulevad elektroonsed liiklusmärgid. – *Eesti Rahvus Rimghääling,* 15. May. Accessible from: https://www.err.ee/595994/parnu-maanteele-tulevad-elektroonilised-liiklusmargid. Last accessed: 05.03.2018.

since they could be conducted with only few key strokes, it is essential to ensure the durability of these systems so the recovery would be swift.

As written beforehand, critical infrastructures, essential services and other crucial services' safety should be shared responsibility of the state and the private entities operating within these domains.[59] To achieve this cooperation, clearly, good legislative initiative must be shown by ensuring transparent and well-functioning law.

Finally, the thesis has arrived at its core. In this thesis, the reader shall be introduced to the complicated balancing act of transparency and secrecy when implementing the new NIS Directive into Estonian law. The reader shall be introduced to the current legislative state and whether the new Cybersecurity Act ensures a good balance between transparency and secrecy.

Additionally, the chapters below will introduce the reader to how transparency is provided in Estonia and whether the new law does a good job at balancing much needed transparency and equally important secrecy. Since transparency is multi-facet issue, the reader shall be introduced to different aspects of transparency which will be described in the coming chapters.

3.3. Transparency and secrecy in legislative procedures and in legislations

In many ways people, citizens, view democracy as a form on leadership, where governmental actions are translucent, clear, necessary and accessible. Additionally, all these properties also make debates, discussions and criticism towards government possible, therefore promoting human rights, good governance and democracy.

[59] van Aaken, A., Wildhaber, I. (2015). State Liability and Critical Infrastructure: A Comperative and Functional Analysis. – *European Journal on Risk Regulation,* Vol. 2 (2015), 244-254, p. 245.

Estonia knows well what it means to exist in a society where opacity has taken over transparent legislative process. For most of the 20th century Estonia was under Soviet Russia governance, which was mostly grappled with legislative favoritism towards the leaders of the Soviet Union. Transparency in legislative process was almost non-existent, and transparent laws were few and far apart.

When Estonia re-gained its independence in August 1991, Estonia set its aims towards democratic governance. From the very beginning of the new era of Republic of Estonia, the then prime minister Mart Laar aimed towards making Estonia into tech-savvy nation. This goal has mostly been reached, with many technological solutions both horizontally and vertically within the government and between the citizens and government(s).

Due to high technological development and growth in Estonia, it is quite easy to ensure the availability of governmental documents. Additionally, many measures have been taken by the Estonian government itself to assure the transparency of draft legislations, existing laws and court cases.

Estonia has implemented many e-government solutions to ensure easy access to information. Any level court cases are freely accessible online. All and any national laws are held at an online database called Riigiteataja.[60] Most legislations online include translations to Russian and English. This has all been done to promote the transparent legislative culture in Estonia.

e-Government solutions simplify granting access to different kinds of information. Free access, in return, helps to ensure and promote transparency, accountability, and of course e-government solutions help to eradicate corruption.[61]

[60] Riigiteataja. – [E-database] www.riigiteataja.ee, (24.02.2018).
[61] Bertot, J. C., Jaeger, P. T., Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social meida as openness and anti-corruption tools for societies. – *Government Information Quarterly,* Vol. 27, 264-271, p. 264-265.

3.4. Information communication technology and legislative transparency

In Estonia, ICT (information communication technology) solutions are used very widely, when publishing governmental legislative process. For example, Estonia has made it possible to observe and track legislative processes through a website called *Eelnõude Infosüsteem* (in English: legislative draft information system).[62] On this webpage it is possible, to get access and read through legislative proposals, amendments from different ministries and third parties who are affected by new legislative proposals (stakeholders). Additionally, citizens can find contact information of all corresponding ministries, and responsible ministry contact information to ask additional questions.

The concepts of transparency and secrecy are, without a doubt, antonyms. These terms have both found its way to contemporary legislative and political processes.[63] It is undoubtedly necessary to balance these two seemingly incoherent notions. Transparency is necessary so there would be highest degree of democracy, yet secrecy is necessary in cases where national security is at stake.

When talking about ICT solutions, which help to ensure transparency of legislative process, one could not forget other important aspect of using ICTs. For example, use of ICTs turning legislative process also raises the efficiency of legislations.[64] This phenomena stems from the fact that a lot of parties can be a part of the drafting process. This can ensure clearness of law, necessity and other important aspects of good legislation. Only transparent and clear legislations can be efficient – this in return can cut down legal costs for people because there are less uncertainties in law.

[62] Eelnõude Infosüsteem (EIS). [E-database] http://eelnoud.valitsus.ee/main#vD40c7z4. Accessed on: 23.02.2018.
[63] Birchall, C. (2012). The Politics of Opacity and Openness. Intorduction to Transparency. – *Theory, Cluture & Society,* Vol. 28, Issue 7-8, 1-19, p. 2.
[64] Voermans, W., ten Napel, H.-M., Passchier, R. (2015). Combining efficiency and transparency in legislative process. – *The Theory and Practice of Legislation,* Vol. 3, Issue, 3, 279-294, p. 283-284.

It is clear that ICTs play a great role when ensuring transparency in legislative process, but there are few other aspects which are necessary as well. For example, it is crucial to have a legislation which is easy to understand and clear in language. Provisions which are simple, straightforward and easily understandable are essential for warranting transparency.[65]

3.5. Language – a tool towards legal certainty

Legislation is clear when an average person can understand it and derive her or his rights and obligations from the law. So language in legislation should be so clear and plain that an average reader would not need special education to clearly understand laws. This clearness can be achieved by using clear language and using same definitions and terms throughout law. This uniform language use should not only be in one legislations, rather uniform language and definitions should be used throughout all legislations connected with each other.

Legal certainty is one of the general principles within the European law and it is closely tied with the principle of transparency. Legal certainty implies that those of whom, who are a subject to law, must know what the law is in order to fully abide and act in accordance. In order to abide to the law, requirements must be met, such as:

1. laws must be public;

2. laws must be definite and clear;

3. legitimate expectations must be protected.[66]

In addition to transparency being a good meter for democracy in a state, transparency also induces economic growth.[67] One cannot doubt the fact that transparent policymaking, clear legislation and over all good governance evoke interest of businesses to expand their businesses

[65] Papaloi, A., Gouscos, D. (2013). Parliamentary Information Visualization as a Means for Legislative Transparency and Citizen Empowerment? – *eJournal of eDemocracy & Open Government,* Vol. 5, No. 2, 174-186, p. 179-180

[66] Maxeiner, J. (2007). Legal Certainty and Legal Methods: A European Aletrnative to American Legal Interminancy? – *Tulane Law School of International Law & Comperative Law,* Vol. 15, 541-607, p. 549-552.

[67] Relly, J. E., Sabharwal, M. (2009). Perceptions of transparency of government policymaking: A cross-national study. – *Government Information Quarterly,* Vol. 26, 148-157, p. 149-151.

to nations with these parameters. Estonia, being a part of world's nations, also thrives to achieve economic growth which would make it more compatible in Europe's market and as well as in the world's market. And as NIS Directive proposal also indicated, the purposes of ensuring high common level of network and information systems security is to enhance the competitive edge of countries, and to achieve as unified level of security in those fields so that entering new markets within the European Union would not come with great obstacles in cybersecurity field.

On the other hand, secrecy often can ensure security.[68] For the NIS Directive, the aim is to ensure security of networks and information systems across the European Union. In that regard it would be fair that Estonia opts to have some secrecy in its national law governing the scope of NIS.

Furthermore, it is important to note that Estonia has a regulation concerning the requirements to involve interest groups and the public, this is in place to promote good legislative practice and transparency. The Rules for Good Legislative Practice and Legislative Drafting of the Republic of Estonia[69] (abbreviated HÕNTE) gives legislative process guidance which is obligatory to follow by all legislative body. Additionally, the before mentioned HÕNTE also imposes an obligation to officiate a regulatory impact assessment, which was done accordance with the law in case of preparing for Cybersecurity Act.

Particularly it is important to remark that as with any European Union directive, the national transposition and new law can only be a clear as the Union legislators have formed their directive.[70] The interconnectedness of European Union legislation transparency and clarity has a direct effect on those two factors in national laws, which are derived from these legislations drafted by the Union legislators, have effect on common market and overall business growth within the European Union.

[68] Peters, A. (2010). Transparency, Secrecy, and Security: Liaisons Dangereuses. – *Rule of Law, Freedom, and Security in Europe,* Vol. 6, 183-243, p. 101-103.
[69] Hea õigusloome ja normitehnika eeskiri. RT I, 29.12.2011, 228.
[70] Hojnik, J. (2016). The servitization of Industry: EU law implementations and challenges. – *Common Market Law Review,* Vol. 53, Issue 6, 1575-1623, p. 1601

3.6. Drafting a new law v. updating existing regulations

In Estonia, all legislative processes begin with so called background research of established laws and whether these in force laws have scope, which is required to regulate whichever field necessary at that time. This strategic question helps to come to a unified understanding whether a new law is necessary or could Estonia, or any state, rely on existing legislation. Relying on in force legislations is also described in law literature as the evolutionary approach.[71]

In a broad sense there are two ways to implement directives from the European Union. First way is to confirm in force laws so that these would be up to bar with new demands set by the Union directive. Second approach to implementation of the European Union directives is to conceive a whole new law, which would regulate particular legal questions.

It is each Member States' own decision which way its nation will transpose the European Union legislators' directives.

In Estonia, a responsible ministry is chosen to do the ground work for new legislations. This choice is based on the responsibility areas of ministries. It is clear that the Ministry of Rural Affairs would not be competent to take responsibility to transpose pieces of legislation concerning cybersecurity issues. In Estonia, Ministry of Economic Affairs and Communication was chosen.

In Estonia, Estonian Information System Authority (hereinafter also EISA) requested an in depth overview and background research of currently in force cybersecurity related legislations. The legal analysis was concluded in October of 2016 by Lextal legal office.[72] The before

[71] Kelli, A. (2015). The conceptual bases for codifying Estonia's IP law and the main legislative changes: From the comparative approach to embedding drafted law into socio-economic conext. – *International Comparative Jurisprudence,* Vol. 1 (2015), 44-54, p. 46-47.
[72] Männiko, M., Maaten, E., Poola, M., Männiko, M., Kinkar, R., Rull, A. (2016). *Kübervaldkonna õigusanalüüs.*Accessible: https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf. Last accessed: 06.03.2018.

mentioned legal analysis of the current state of legislations in Estonia follows the good rule of transparency in a sense that it is freely accessible to all interested parties.

3.7. Legal analysis of Lextal law office

The legal analysis conducted by Lextal law office cover all the most important aspects of applicable laws in cyberspace and cybersecurity. Most importantly it answers the question of whether it would be sufficient to only amend old regulations or would it be more rational to draft a completely new law which would secure network and information systems security in the Republic of Estonia.

Firstly, it is clear that one of the first factor which would ensure clarity and transparency is the commonly used language and unequivocally understandable vocabulary. When familiarizing with the legal analysis[73] conducted by Lextal law office it becomes very clear that Estonian national legislations lack indisputable common language when it comes to new-age cyber vocabulary. The need to have harmonized cybersecurity related vocabulary must be a long term goal,[74] every new legislation should commend to same definitions.

The issue of lack of common terms would bring many issues in transparency. Rather, the lack of common language would promote concealment. This would result in a small circle of people who would have the knowledge and could force hands in issues which would not actually fall within the scope of cybersecurity nor network and information systems security. Additionally, obligated parties under the current legal order would not be as well informed of their responsibilities as they ideally should be.

For an effective legislation it is imperative to have transparent and unified language used in regulations. Unified language use across board would ensure best application of duties and

[73] *Supra nota.*
[74] Luiijf, E., Besseling, K. (2013). Nineteen national cyber security strategies. – *International Journal of Critical Infrastructures,* Vol. 9, No. ½, 3-31, p. 25.

rights to the affected parties. Thus far Estonian legal order has not implemented unified understanding of cybersecurity related language.

To illustrate, there is no unified idea within Estonian national legislations which would clearly define what is cybersecurity, what are cyber threats or even what cyber overall is, how will certain actions within the cyberspace trigger security actions and so on.

While, for a legislation to be clear, not only does the language need to be unified, the roles of affected parties must also be set in place. Their responsibilities must be set in a clear way where there is small room left to err away from applicable duties. The obliged parties also include government's agencies.

Estonian's national regulations have set quite clear guidance for governmental agencies when it comes to ensuring cybersecurity. The exception in this case would be Estonian Information System Authority, which is a central information systems authority within the nation.

The Estonian Information System Authority's role was up for great discussion since its role within the NIS Directive would be substantially greater than it has been thus far. The *de facto* EISA has been the supervisory authority in Estonia, but there has been no set regulation which would ensure their enforcement powers nor their right to request information and sign disciplinary penalty.

This lack of regulation would make the enforcement of NIS Directive aims and objectives practically impossible. Since the supervisory authority would have to be in a legal standing where it is free to ask necessary investigatory information and fine entities which do not comply with their obligations.

The argument for a new law would come just from the fact that EISA has no disciplinary power set out in current legislations. A new regulation would allow to furnish EISA's rights, duties

and disciplinary measures with a higher accuracy. This would support the transparency of enforcement and would lift a cloak of secrecy off from the disciplinary part of NIS Directive.

In addition to the before mentioned issues, EISA thus far has lacked the authority to be involved in cybersecurity incidents. At the present time, only two obligated parties are liable to notify EISA of cybersecurity incidents. These two parties are communication companies[75] and so called trust service providers which offer e-identification and e-transactions.[76] This again, would greatly impede the authority of EISA if they are not duly notified and involved when a cybersecurity incident takes place.

In accordance with the intentions of the draft to work out a cyber-domain legislation[77], at the present time Estonian national legislation lacks the obligation to notify EISA of cybersecurity breaches by the public sector and by the vital services providers. Additionally, it is important to note that notification obligation may breach third party rights, therefore notification duty must be unequivocally set in law in accordance with the Constitution of the Republic of Estonia paragraph 3 section 1.[78]

Moreover, there is no regulation on how and for which purposes cybersecurity notification information could be used by EISA. The only guiding document in that aspect is EISA's statute.[79] But this document is not applicable for anyone else outside EISA, so this could ripple into a much greater problem.

The before mentioned aspects only highlight the need to implement new regulation into Estonian national legal order. The notification obligation must be set in law in a way where it is indisputably applicable to obligated parties. Only this way could Estonia support the European Union legislators' which to have more cooperation between Member States. If

[75] Electronic Communications Act, RT I 2004, 87, 593, § 87^2
[76] Electronic Identification and Trust Services for Electronic Transactions Act, RT I, 25.102016, 1, § 4
[77] Majandus ja Kommunikatsiooniministeerium. *Kübervaldkonna seaduse väljatöötamise kavatsus.*Accessible from: http://eelnoud.valitsus.ee/main/mount/docList/3529d47c-0b7c-4f39-9003-4a839a7d8c49#goFNzNsW, 09.03.2017. Last accessed: 06.03.2018
[78] The Constitution of the Republic of Estonia, RT I, 15.05.2015, 2.
[79] Riigi Infosüsteemi Ameti põhimäärus, RT I, 28.04.2011, 1.

Estonia lacks regulations obliging private entities to report cybersecurity breaches than the nation would be obstructed from playing its part in European wide cooperation.

Furthermore, the current legislative state has made Estonia's information systems security management responsibilities somewhat fragmented. This fragmented approach would need to be harmonized. Not only is there an issue with the fact that not all entities and service providers get their security obligation information from different and wide set of legislations, but there also lacks a uniform approach to these measures. This fragmentation leads to complex situation where there is difficult to orient for entities and service providers.

To illustrate the before written problem, few examples are necessary. The vital services providers are obliged to notify under the Emergency Act[80], which provides that all vital service providers are required to warrant the security of information systems which are used in regard to providing vital services. The Emergency Act § 41 section 3[81] provides that information security measures shall be laid down by regulation the Government of the Republic. So in a sense, providers of vital services come to a point where they need to be familiar with two different set of regulations, first with the Emergency Act and secondly with government's regulation which lays down specific requirements.

Additionally, communications companies, broadcasting network and critical communications, maritime communications and operational radio network service providers are obliged under the Electronic Communications Act.[82] In addition to these communication network providers, under Estonian national law in force right now, the notification duty expands also to railway infrastructure and railway vehicle owners under the Estonian Railways Act[183], and also to port service providers and port operators under the Ports Act.[84] In addition, under the Aviation Act[85] the cybersecurity breach notification duty extends to quite a wide scope of subjects. These subjects include subjects associated with the operation, manning, manufacture and maintenance

[80] Hädaolukorra seadus, RT I, 28.12.2017, 49, § 41.
[81] *Ibid.*
[82] Elektroonilise side seadus[1], RT I, 01.07.2017, 2.
[83] Raudteeseadus, RT I, 16.05.2017, 3.
[84] Sadamaseadus, RT I, 03.03.2017, 24.
[85] Lennundundusseadus, RT I, 03.03.2017, 16.

of aircraft, and the providers of air navigation services, the operators of aerodromes and heliports, and the training of aviation specialists.[86]

Thus far the argumentation has found that the current Estonian legislative sphere has very fragmented approach to cybersecurity.

Firstly, there is an issue with furnishing national legislations with uniform cybersecurity related vocabulary. Thus far many national regulations use different terms[87] to describe essentially the same aspects – this causes confusion and promotes lack of transparency.

Secondly, the reader has been given an overview of EISA's lack of legal grounds to enforce necessary obligations under the new NIS Directive. Even though EISA is *de facto* and *de jure* agency which duty is to handle cybersecurity incidents and has a supervisory competence over some service providers.[88] In addition, reader was introduced to the constitutional problem when there are to set regulations when subpoenaing information from service providers.

Thirdly, the current legislative state in Estonian national laws leaves quite a fragmented approach to who and when should report cybersecurity incident information or suspected breach notification.

As a result of the all before written factors it seems pretty clear that new legislation should be favored. New regulation would help smooth out the differences and would bring more clarity to all involved parties. While it may seem drastic measure to have a new regulation implemented from scratch to transpose European Union directive, it does seem the most

[86] Lennundusseadus, RT I, 03.03.2017, 16, § 1 section 2.
[87] Männiko, M., Maaten, E., Poola, M., Männiko, M., Kinkar, R., Rull, A. (2016). *Kübervaldkonna õigusanalüüs.* Accessible: https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf. Last accessed: 06.03.2018.
[88] Majandus- ja Kommunicatsiooniministeerium. (2017). *Küberturvalisuse seaduse eelnõu seletsukiri.* Accessible from: http://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b#90L0yx37. Last accessed on: 06.03.2018.

reasonable route to take. Moreover, this is reasonable due to the fact that Estonia thus far has had no special regulation concerning cybersecurity while being e-nation.

NIS Directive obliges the MSs to establish national strategies which concern cybersecurity. Estonia is one of the only few European Union nations which has a strategy concerning cybersecurity related issues and public-private partnership.[89]

To highlight the issues in current Estonian national legislations, when it comes to regulating network and information systems to extent which is necessary under the scope of the NIS Directive, few more examples could be brought out. These illustrations will exemplify why the choice of drawing up a completely new regulation was and still is the right decision.

Firstly, the NIS Directive Article 15[90] lays down the obligation to have set security auditing rules. Thus far Estonia does not have necessary national regulations which would obligate operators of essential services to carry out such security auditing. To implement the NIS Directive appropriately in Estonia it is certain that such obligations must be laid down by law and enforcement measures for this obligation as well.

Further, at the current time there are problems with obligations to local governments and public authorities to ensure security measures. At the present time the only pieces of regulation and act which regulate their obligations on that field are Public Information Act[91] and Information Systems Security Measures System Act[92] (hereinafter also referred as ISKE). Under the before mentioned regulations the local governments and governmental institutions must ensure appropriate level of security to their information systems with state of art security measures.

[89] Turcu, D. (2016). Considerations on cyber security legislation and regulations in Romania.- *International Scientific Conference ''Strategies XXI'',* Bucharest. Bucharest: National Defence University, 173-180, p. 174.
[90] The European Parliament and the Council of the European Union (EU) No 2016/1148 of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union, OJ L 194/1.
[91] Avaliku teabe seadus, RT I, 04.07.2017, 11.
[92] Infosüsteemide turvameetmete süsteem, RT I, 2007, 71, 440.

It is worth to highlight that there have been interpretation issues concerning ISKE regulation. That point has also been brought out by the National Audit Office of Estonia in its 2014 annual report to Parliament.[93] Some issues which were highlighted were the fact that information systems definition has not been defined to the point where it would be clear which systems are the object of ISKE regulation. Moreover, in ISKE regulation it is also hard to get a clear view of who is the subject of this regulation. This has brought local governments and governmental institutions to a place where there is no clear way of enforcing ISKE within their work.[94]

Further, under the NIS Directive CSIRT's are introduced to many new objectives. Some of these include for example organizing monitoring, early warnings notification in case of risks and cybersecurity incidents and also more of an overall awareness raising. Awareness raising can bring many benefits, since the end users of network and information systems are in fact humans, who undesirably will be the biggest victims of cybersecurity related incidents.[95] Especially this can be the case when online banking systems are being breached, but also the nations itself can become a victim of cybersecurity breach.[96] But in order to be best prepared and protected from potential disturbances there must be a trust between the agency which is gathering information and of course legal obligation for private entities to share sensitive information.[97]

In addition, CSIRT's shall be responsible for analyzing information related to cybersecurity incidents and as well as reacting to incidents where and when necessary. Thus far Estonian national regulation has subjected EISA to dealing with cybersecurity incidents if these incidents could bring imbalance in public order or incidents which require swift reaction. Although some legislation in intact, Estonian national regulations still lack clauses which would permit EISA and CERT EE to ask out log-data.

[93] Riigikontroll. (2014). Ülevaade riigi varade kasutamisest ja säilitamisest 2013-2014. aasta. [Online] http://www.riigikontroll.ee/Riigikontrollipublikatsioonid/Riigikontrolliaastaaruanneparlamendile/tabid/110/ItemId/434/View/Docs/amid/732/language/et-EE/Default.aspx. Last accessed: 07.03.2018.
[94] *Ibid.*
[95] Scheau, M.-C. (2017). Strategic Management of Critical Infrastructures and Financial Domain. – *International Journal of Information Security and Cybercrime,* Vol. 6, Issue 1/2017, 13-24, p. 15-17.
[96] Manley, M. (2015). Cyberspace's Dynamic Duo: Forgning a Cybersecurity Public-Private Partnership. – *Journal of Strategic Security,* Vol. 8, No. 5, Article 9, 85-98, p. 91-93.
[97] *Ibid.,* p. 91-93

Without the right to ask log-data about cybersecurity incidents it would be beyond the bounds of possibility to analyze cybersecurity incident data and have defensive measures intact in case of other similar cybersecurity breaches. The same fact would make it impossible to promote cross-European cybersecurity incident information flow – Estonian national authority would have no useful information to share.

Thus far, Estonian national law obliges electronic communications entities to disclose log-data under the Electronic Communications Act § 111[198] under very specific circumstances. Electronic communications entities must release log-data, for example to Financial Inspections, Data Protection Inspectorate, the Prosecutor's Office, and so on, but thus far EISA is not among those of whom who are listed. To a certain extent this kind of limited subject circle cuts down the chances of data leak, which could in return affect not only the companies but also their end-users. As a result of a chance of leakage, there must be also set standards on how incident data can be processed and by whom the processing can be done.[99] Whether it is wanted or not it must be remembered that incident information can and will contain personal data, to which personal data processing regulations and security measures shall expand. Though amongst personal data, it cannot be forgotten that sensitive business information can be considered confidential, therefore handled with care and erased when no longer necessary for which ever purposes data was gathered at the first place.[100]

In addition to the all before mentioned issues, Estonian national regulation lacks legislation in whole on the field of IXPs, domain name systems (abbreviated to DNS) and on top-name domain registry (abbreviated to TLD). The same conclusion was drawn in Lextal law office's cybersecurity field legal analysis.[101]

[98] Elektroonilise side seadus, RT I, 01.07.2017, 2.
[99] Cormack, A. (2016). Incident Response: Protecting Individual Rights Under the General Data Proetction Regulation. – *Scripted,* Vol. 13, Issue 3, 259-282, p. 259-261.
[100] van der Sloot, B. (2015). Do privacy and data protection rules apply to legal persons and should they? A proposal for two-tier system. – *Computer Law & Security Review,* Vol. 31, Issue 1, 26-45, p. 41-43.
[101] Männiko, M., Maaten, E., Poola, M., Männiko, M., Kinkar, R., Rull, A. (2016). *Kübervaldkonna õigusanalüüs.*Accessible: https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf. Last accessed: 06.03.2018.

Based on the before written argumentation it becomes apparent that Estonian national regulations do not fulfill the obligations which arise from the NIS Directive. As a consequence, new law must be drafted and approved to comply with necessary standards set out by the European Union legislators in the NIS Directive.

4. ESTONIAN CYBERSECURITY ACT – BALANCING TRANSPARENCY AND SECRECY

4.1. Transparency

Firstly, before this thesis will go any further it is important to discuss what transparency means. At least what this (legal) principle means in this thesis. Additionally, it is imperative to choose which aspects of transparency and secrecy is written about, since transparency norms could be applied to the legislative process and as well to the regulation itself.

Transparency tends to have undefined scope – it is free for interpretation, depending on specific circumstances. Transparency principle could be seen as an umbrella term, which embodies many notions. Even though transparency leans towards uncertainty, it is closely tied with the essence of democracy.[102]

In addition, transparency could mean that documentation and decision making procedures are accessible – this promotes transparency as well. This access based transparency is relatively easy to do, especially in a tech savvy nation like Estonia. Thankfully, Estonia has developed information systems, which are easily accessible and where legislative process can be tracked at all times.

In this thesis transparency shall be understood as clarity of structure of Cybersecurity Act, language use in the new regulation and as well as how well are roles defined in the new draft legislation. And whether the responsibilities in case of infringements are clear.

The clear drafting of legal norms plays great, if not the most important role in regulations. Clarity in regulation leads to legal certainty, which could be considered one of the key factors

[102] Bradley, C., M. (2012). Transparency and Financial Regulation in European Union: Crisis and Complexity. – *Fordham International Law Journal,* Vol. 35:117, 1171-1206, p. 1172-1174

of democratic society. To guarantee legal certainty, regulations should be clear and understandable and have a logical structure.

Estonia, as the European Union MS is obliged to transpose the Community law to its national law. Every transposition and implementation must also be made with certain precision. National legislators must ensure that provisions of the Community law are transposed with clarity and transparency in mind to fully comply with the set European Union law.[103]

As mentioned beforehand, Estonia has successfully developed information system which enables the people to track legislative processes. This is a positive step towards securing transparency and openness towards the people and other affected parties such as legal entities.

4.2. Limitations to transparency

Transparency may be limited and in return regulation could be covered necessary secrecy.[104] Limiting may be done in a way where transparency is unexplainably being swapped with secrecy for the benefit of the government not for the benefit of national security, citizens nor for overall societal well-being.

The necessary limitations to transparency may stem from data protection rules, national security issues, state secret, copyright regulations, and of course from commercial codes. All these aspects need to be taken into account when assessing the need for secrecy.

In Estonia there is a national legislation which governs which documents must be ensured with proper secrecy and security. In Estonian State Secrets and Classified Information of Foreign States Act[105] governs how and which kind of documentation are deserving of higher or highest

[103] Vlaicu, A.-M. (2011). Effectivness of EU law in member states. – *Lex ET Scientia International Journal,* Vol. 18, Issue 1, 162-173, p. 167-171.
[104] Barnard-Wills, D. (2013). Security, privacy and surveillance in European policy documents. – *International data Privacy Law,* Vol. 3, No. 3, 170-180, p. 174-178.
[105] Riigisaladuse ja salastatud välisteabe seadus, RT I, 05.05.2017, 5

degree of protection and restriction rules. Under this national law, not all information can be accessible to the public nor to persons who have not been granted access rights within an organization. This legislation makes restriction of transparency legal in some cases.

4.3. Secrecy in cyber- and national security

When one would think about security they could easily in parallel think of secrecy. Information which is kept secret cannot become security issue, since there are limited number of those how possess necessary information to cause insecurity.

Often confidentiality is used in employment contracts to keep delicate information secret.[106] Such delicate information often includes data about production or business secrets. Confidentiality clauses are commonly used to protect businesses from having their most valuable information leaked.

So, secrecy is necessary to conduct business and to, of course, to have security that information one has deemed confidential will have protection.

In cybersecurity, secrecy can mean two things:

1. it could mean that governments, businesses, authorities or other agencies use secret computer code to keep track and spy after citizens; or

2. it could mean that an entity does not give out their system description, computer code, and other such information to not let hackers and other malicious actors to take advantage of their product or their weaknesses.

Secrecy clearly has its advantages, it can be a way that helps secure systems, networks and citizens from malicious activities. At the same time, secrecy which has no justification, or at

[106] Töölepingu seadus § 22, RT I, 28.12.2017, 43.

least clear justification, could be seen as private entities having too much of a freedom to offer security they seem fit. This security may not always be up to bar to what is expected from them and clients and citizens are left to trust their word.

Obviously in national security there must be a certain extent of secrecy. This seems clear and logical, since government would not like its security measures be available to aggressive states. It is clear that cybersecurity is undeniably an integral part of national security, therefor some degree of secrecy is considered fit. But legislators cannot hide behind the national security claim, when leaving too many unanswered questions open and not regulating with a degree of certainty.

Secrecy and transparency must work together to achieve the best result possible, especially in important aspects like national and cybersecurity. When these principals are balanced, the outcome is what all nations want to achieve – good public-private cooperation, safe networks and information systems and protected citizens.

4.4. Balancing transparency and secrecy

Only when secrecy and transparency are balanced can there be as optimal regulation as possible. Without any transparency there would be no control and partnership between private and public parties. On the other hand, same could be told about secrecy, without any secrecy there could be no effective defensive legislation nor, again, trust between parties because some secrecy principles must be ensured.

In the case of Cybersecurity Act, it is clear that the subject of the regulation, must be in safe enough zone to willingly, and sometimes maybe not so willingly, hand over very sensitive information concerning their security measures, cybersecurity breach logs, and other related documentation. To have free flow of information, trust must be on both ends, but especially on the side of private parties who trust this sensitive information to a governmental authority. Not

to mention that EISA could have remote access to network and information systems in order to remedy direct high risk or disturbance.[107]

Public authorities are among the prime processors and even creators of data.[108] The data created and processed include, but are not limited to, mundane weather data, tourist data, education quality data, but also to data about national security and with Cybersecurity Act also data about cyber-security incidents.

To add to these domains, the information about cybersecurity breaches, suspected or related breaches it adds up a very large proportion of data processed, gathered and stored by government and its agencies. This large amount of data would all need information systems itself, appropriate security regulation, and management. In addition to cybersecurity incident information processing being delicate, the processing personnel must be equipped with necessary expertise.[109]

4.5. Balancing transparency and secrecy in Cybersecurity Act

To start off analyzing Estonian Cybersecurity Act one of the first things to note is the fact that the new regulation is mere 28 paragraphs long. In comparison, the Estonian National Defiance Act[110] is more than 90 paragraphs long. From this, it is fairly obvious that the legislators have wanted to cram the whole cybersecurity related aspects to as short as possible regulation. The mere shortness of the law gravitates towards opaque regulation and many uncertainties which may lead to violations even of the rights granted by the Constitution of the Republic of Estonia, more specifically the right under the paragraph 15 of the Constitution.[111]

[107] Vabariigi Valitsus. Küberturvalisuse seaduse eelnõu § 16
[108] Janssen, M., Charablabidis, Y., Zuiderwijk. (2012). Benefits, Adoption Barriers and Myths of Open Data and Open Government. – *Information Systems Management,* Vol. 29, No. 4, 258-268, p. 259-260.
[109] Raab, C., Szekely, I. (2017). Data protection authorities and information technology. – *Computer Law & Security Review,* Vol. 33, Issue 4, 421-433, p. 421-423.
[110] Riigikaitse seadus, RT I, 27.06.2017, 6
[111] Eesti vabariigi Põhiseadus, RT I, 15.05.2015, 2.

On the other side, the shortness of new legislation could also try to show that everything is easy, clear and easily enforced. To keep new legislation short might be a try not to build up too much confusion and over-juridical text.

In the new Cybersecurity Act draft,[112] the used language is not too complex. The draft beings with giving explanations to definitions used in the new regulation. Amongst listed definitions there are given explanations to words such as ‘’network and information system’’, ‘’security of a system’’, and so on. This explanatory paragraph is clearly added to make the reader of the regulation aware of new subjects and objects of regulation, and to ensure that all people would understand these unequivocally.

4.5.1. Operators of essential services

Further, the new Cybersecurity Act draft § 3,[113] gives explanatory description of whom are considered to be operators of essential services. For example, there are no exact commercial entities named to be the operators of essential services, rather the regulation gives room for interpretation based on certain criterions which entities must fulfill to be considered operators of essential services. The quantitative and qualitative criterions leave little room for secrecy, rather these promote transparency amongst operators and obligated parties.

If one would view it on the side of secrecy, it is good that there has not been named any certain subjects of regulation because it leaves room to interpret the regulation in accordance with situations at hand. In the case where a regulation would name certain service providers, there would be no flexibility to a regulation.

[112] Majandus- ja Kommunicatsiooniministeerium. (2018). Küberturvalisuse seaduse eelnõu. [Online database] - http://eelnoud.valitsus.ee/main#Bm8zkbOF. Last accessed: 09.03.2018.
[113] Vabariigi Valitsus. Küberturvalisuse seaduse eelnõu. § 3

Though, Estonian national regulation draft says that it shall be in EISA's duties to identify such operators of essential services. So, no commercial entity will not need to inform EISA if they fall under these categories.

Additionally, the draft regulation implies that this operators list shall be renewed in every two years. Unfortunately, the draft does not give a clear view of which rank EISA's employees shall make these kind of decisions nor is there implications whether these kind of decisions can be overturned. This makes transparency on decision making much smaller, since there is no legal specification on circle of people who will be making decisions. In the author's opinion there is no need to keep the circle of people making such rulings a secret, rather it should be public knowledge who makes such decisions.

Additionally, Estonian Cybersecurity Act draft gives no implication whether the list of these operators will be made public and if they are which communications route they will be communicated. If the list is not made public could an average citizen request information about this data or will it be considered classified information. To some extent, classifying this data would make sense, since it is possible operators would become a greater target if cybercriminals would get access to this information.

4.5.2. Digital services providers

Additionally, the fact that the new draft law will not apply to digital services providers, which do not have at least 50 employees and whose annual balance sheet total or annual turnover is not at least 10 million euros. This means, that both 50 employees and at least 10-million-euro turnover must be present for the law to be applicable, this means that entities may start to write off workers to other entities within the group to not be a subject to the new law while still having a turnover over 10 million euros. This would mean that there would be persistent threat within the networks and information systems if these companies decide not to comply. This could be especially an issue in Estonia, where there can be small employee number, while still making huge profits and governing a large portion of the market share. But at the same token, it could

be seen as sheltering small businesses which would struggle to meet the security measures which are required.

The question rises about the classification of gathered data – will cybersecurity related information, such as log files, be classified by using principles described in State Secrets and Classified Information of Foreign States Act?[114] This question has left unanswered by the Estonian draft legislation. Leaving this important question unanswered may raise many concerns for entities who are under the obligation to share cybersecurity related information because that would mean that information about their clients (especially natural persons), security measures, security threats, and other sensitive business information would possibly be left unprotected. Under the Estonian Competition Act[115] every entity has the right to have its business secrets protected, this includes protected against forceful publication and sharing of such information by government and its' agencies.

Additionally, there being no information whether any classification of information shall be made nor on what basis any classification will be made, there is also no reference to as to whom will be in charge of deciding whether, for example Eesti Energia cybersecurity logs which go back let's say 4 months will be classified. For EISA employee who is in charge of classification might not understand the importance of information to Eesti Energia and might sign the information with the lowest degree of protection, while a board member of Eesti Energia would disagree with this classification standard completely because (s)he sees this information as something that would possibly open doors for competitors to gain advantage.

But at the same time, even though Cybersecurity Act does not give exact guidance on how data will be classified, there might be inner-EISA classification guide which will regulate on which principles classification is enforced. This may help entities, who themselves cannot designate a classification on their data, to keep it secret. And of course, EISA's inner manual could also keep entities from ''over protecting'' information. If every entity would claim that log data is

[114] Riigisaladuse ja salastatud välisteabe seadus, RT I, 05.05.2017, 5
[115] Konkurentisseadus § 63, RT I 20.12.2017, 7.

confidential then no effective information exchange could take place neither on national level nor on European Union level.

In addition, in § 4 of the new regulation,[116] the legislator has given definition to digital service providers. When in the paragraph governing the operators of essential services gives many qualitative and quantitative criterions to ascertain these, the regulation leaves wide interpretation room for digital services providers. Under the new regulation whoever offers online market place, online search engine service or cloud computing service fits under the scope of the new regulation. The same questions rise here – will the list of these online market places, search engines and cloud computing services made public or will it be a closed list to which access is granted on need-to-know basis. Some additional factors and uncertainties appear here also, for example shall these service providers themselves get notified that they belong under the scope of the new law or will every entity need to carry out applicability analysis and then decide themselves and give notice to supervisory authority/authorities.

It is though justifiable that the list of operators would be kept secret. Obviously announcing and keeping an open-end list available online could make these operators more of a target for malicious attacks. To illustrated, lets imagine that Eesti Enrgia is put on essential operators list. Malicious hacker from anywhere in the world could gain information that Estonia looks at this service provider as an essential operator. It would make Eesti Energia a simple target to cause a lot of disruption. With keeping a public open-end list would mean that malicious actors from even Caribbean Islands could make a very targeted attack on Estonia through attacking one of essential service provider.

4.5.3. Public-private co-operation

Both the NIS Directive and Estonian draft legislation call for co-operation amongst public and private sector. Estonian draft beautifully establishes such co-operational duty, but unfortunately it fails to specify some important aspects of co-operation. Such aspects include, whether there

[116] Majandus- ja Kommunicatsiooniministeerium. (2018). Küberturvalisuse seaduse eelnõu. [Online database] - http://eelnoud.valitsus.ee/main#Bm8zkbOF. Last accessed: 09.03.2018.

would be any consequences to non-co-operation, what are the time limits to how quick does an entity need to provide any information, access or assistance. Without regulating these aspects there will be very fragmented approach from companies when following their obligations, some may report as soon as possible or as soon as they have knowledge, while many may err away of any notification and just deal with the aftermath of consequences since there is no guarantees that information that they share will be safe and secure.

Co-operational assistance which is required by the draft law, could include giving remote access to networks and information systems. Thus far Estonian Electronic Communications Act has established very strict rules for electronic communications service providers, who are under the obligation to keep year-long logs about communications, and moreover the Electronic Communications Act § 112[117] makes it clear that with a contract Police and Border Guard have the right to real-time logs for online detection of terminal equipment used on the mobile network. But there is a catch – there has to be a contract, so to certain extent these service providers are not under strict obligation rather they are free to step into an agreement. Under the § 16 of the draft law, it is clear that EISA would have remote access to network and information systems of service providers across Estonia who are within the scope of Cybersecurity Act. This again raises many security, secrecy and capacity questions for private entities. As this thesis has used Eesti Energia as an example beforehand, it will continue. It is hard to imagine an employee of EISA having enough knowledge to take over the whole system, or even a part of a system, of Eesti Energia. Firstly, this employee might lack any knowledge about how these systems are built up, how they function in reality and whether these systems have something wrong in them or not. This could lead to a situation where EISA's employee overreacts and acts with way more intrusiveness than actually necessary – this again could lead to a situation where Eesti Energia loses profit, gains a bad reputation amongst clients and so on.

As described beforehand, EISA's access rights raise big issues, especially when there are decisions involved which are too overbearing. Unfortunately, Estonian draft law does not bring out any kind of remedies if EISA does not comply with the law, or even what is considered over stepping their rights. From the perspective of transparency, it is hard to not see it as an

[117] Elektroonilise side seadus, RT I, 01.07.2017, 2

issue that a legislation gives powers but does not have any remedies to contain the actions of EISA.

The fact that the draft legislation seems to lack any kind of repercussions for the governmental institutions in situations where they might step over their rights and start violating the rights granted to entities or even the rights of citizens and residents. Under the Constitution of republic of Estonia, everyone has the right to recourse in court,[118] this right must always be ensured. In the Cybersecurity Act there are no measures written, which would ensure this right nor any other alternative dispute resolution measures neither, moreover there are no clear definitions on what would be considered as a violation of EISA's rights to act.

It is apparent that draft law lacks clearly defined responsibilities for EISA. The draft inadequately leaves out the legal remedies for entities who belong under the scope of Cybersecurity Act.

Then again it is understandable that EISA does not have clear responsibility outlined in the Cybersecurity Act. This is because of the risk that entities would start claiming for damages, this in return would mean that EISA would most likely be apprehensive about taking action. If there is likelihood of having monetary responsibility, private companies could spend thousands upon thousands of euros in legal fees, time on lobbying and so forth to claim for damages, which would be most likely too overbearing on governmental agency like EISA. To keep networks and information systems secure and under control of EISA it makes sense, that responsibility of EISA is not mentioned.

In addition, if legal remedies are not highlighted in the Cybersecurity Act it could be because Estonian court system is already so over-worked that adding load of cybersecurity related issues on the table would only complicate the issue.

[118] Eesti Vabariigi Põhiseadus § 15, RT I, 15.05.2015, 2.

In addition, the draft of Cybersecurity Act includes a clause which puts a duty of co-operation on the subject of the draft law. Paragraph 6, point 4[119] sets out the before mentioned obligation but it does not define what is considered to be a co-operation nor does it set a time limitations within which entities and institutions need to co-operate. While entities are obliged to notify EISA of breach within 24 hours after gaining the knowledge of a considerable incident, there are no clauses which would specify time limits for co-operation. This could lead to a situation where entities will co-operate after the fact, rather than turning a breach within their systems.

At the same time, co-operation could mean set of completely different actions in various cybersecurity related breaches. So one could argue that the reason Cybersecurity Act is opaque on that issue is the reason that it could mean so many different things. In one cybersecurity related breach co-operation could mean only notification of a breach, code of the computer worm that set off the breach and that is it. In other cases, co-operation could mean something completely different, like granting access to EISA CSIRT team, which would help to resolve and remedy any suspicious actions within the network or information system. On this view, opaque regulation is rightful choice, because it leaves wide interpretation room for each individual breach.

As mentioned before, the draft law does not really set clear standards on what is considered a co-operation. Co-operation could be interpreted in many ways, would it be granting access to systems and network, or would it be giving log information after the fact, if so where would log info end up and on what basis is classification assigned to the logs. In addition, the draft law gives no guidance on what would non co-operation be considered and what would be the legal repercussions of such behavior. The entities are left to decide themselves what is and what is not co-operation, this in return defeats the purpose of NIS Directive and Cybersecurity Act.

[119] Riigikogu. Küberturvalisuse seaduse eelnõu. [Online] - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59. Accessed on: 20.04.2018.

4.5.4. Partial implementation

One more important thing about Cybersecurity Act that must be highlighted is the fact that Estonia is only partially implementing the NIS Directive. The partial implementation could also be considered one of the weak points of the European Union law, since growing number of legislations coming from the Union the Member States are struggling to keep up with the pace, this can result in partial implementation of the Union law, which may defeat the initial purpose.[120] The NIS Directive calls for the Member States to have national cybersecurity strategy and it has specific points which need to be covered with national strategy. Unfortunately, Estonian draft law is completely missing any mention of national cybersecurity strategy. Regrettably with this Estonia might conflict with the European Union treaties, which establish obligations to transpose directives in full. Without national cybersecurity strategy clauses, it is hard to assess whether or not Estonia fulfills its obligations and set standards in accordance with the NIS Directive.

On the other hand, it is wise not to have every cybersecurity related aspect, especially when talking about national strategy points of cybersecurity, in one regulation. Firstly, it is wise not to have national strategy key aspects in the law because that would make some points of Estonian national security strategy known for everyone in the world, especially since all Estonian national laws are freely accessible in English, Estonian and Russian. Secondly, it is much wiser to keep cybersecurity related national strategy in a completely different document, which is classified to be used only within the Justice Ministry and by national security strategist. Especially when one would look at the Cybersecurity Act it is clear that this act only aims towards private sector and few governmental agencies such as Estonian Public Broadcasting, it would make a really complex regulation if national cybersecurity aspects would be added to this. For legal clarity it is much more transparent and reasonable to have a completely different document for such strategy.

[120] Dimitrakopoulos, D.G. (2001). The Transposition of EU Law: 'Post-Decisional Politics' and Institutional Autonomy. – *European Law Journal,* Vol. 7, number 4, 442-458, p. 443-446.

4.5.5. EISA's powers and responsibility

Estonian draft law requires EISA to receive monitoring information and have capacity to supervise that entities comply with the standards and measures written down by Cybersecurity Act. As mentioned beforehand, at this time the Electronic Communications Act paragraph 112[121] regulates how and under what circumstances law enforcement agencies can get access to real-time identification of location of terminal equipment used in mobile network. This information can only be made available if the parties have stepped into a contract. Unfortunately, Cybersecurity Act gives no information about on what legal grounds should entities share information – would entities be able to step into willing agreements or will this information sharing be legally obligatory – this question has left completely unanswered by the new draft law.

At the time where all people, entities and governments are dealing with greater and greater number of data, the new draft law requires EISA to keep another database concerning cybersecurity related incidents and log data concerning these. Under the general Data Protection Regulation,[122] if an entity processes any sort of data concerning identified or identifiable natural person they are under the obligation to follow the processing rules of the before mentioned regulation. Regrettably the new draft law does not give any specification on what are the retention periods for collected data and what data points exactly are kept. There is no justification in legal texts which would promote unspecified data retention periods. These under regulated areas can cause massive concerns to EISA – not only is it burdensome to keep all data, it can become a cybersecurity risk within itself.

Moreover, it is very important not note that the new Cybersecurity Act has no mention of EISA as an essential service provider. In Estonia EISA is the provider of X-road, which is an essential part of e-services, and the provider of data communication network for public authorities (in Estonian known as ASO network). X-road and ASO and two of the most essential services in

[121] Elektroonilise side seadus, RT I, 01.07.2017, 2

[122] The European Parliament and the Council of the European Union (EU) No 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 04.04.2016.

Estonia, and many other services are connected with these, it would only make full sense if EISA would also fall into the category with the obliged parties.

While EISA itself is an essential services provider, it is the agency under the Estonian law to be the supervisory authority. If EISA was, rightfully, an obliged party and the supervisory authority it would go against the Constitutional idea of separation of powers.[123] It is the author's opinion that EISA has been left out of the draft law without correct consideration of its importance in providing essential services across the nation, horizontally as well as vertically. EISA should be a part of the obliged parties and fulfill the measures drawn down by the Cybersecurity Act.

Additionally, EISA should be a subject of new Cybersecurity Act especially now that the agency is on the verge of getting access, collecting, storing and processing cybersecurity related data. It has no justification that EISA is left out of the new legislation. This only cloaks the new legislation with more uncertainty, therefor with unnecessary secrecy.

Last but not for least, the Estonian draft law gives EISA the power to give itself authority to perform some law enforcement actions. Under the Law Enforcement Act[124] the law enforcement agency is the police, which act under the regulation of state authority, which in Estonia is Ministry of Interior. Following that logic, cybersecurity related violations and monitoring fall within the power scope of the Ministry of Interior and permissions to use special measures should fall under the responsibility of prosecutors and courts.

In conclusion, it is the author's opinion that the new Cybersecurity Act lacks transparency in many parts. Such parts include security of log data, rights and obligations of RIA and other issues as written beforehand.

Some of these transparency issues cannot be justified with the need to balance secrecy. Entities have the right to know where their network and information systems data end up, moreover

[123] Eesti Vabariigi Põhiseadus § 4, RT I, 15.05.2015, 2.
[124] Korrakaitseseadus § 6, RT I, 02.12.2016, 6

citizens and residents of Estonia have also the right to know where their data might end up. Nonetheless, people and businesses need to be ensured that their data, which ever data might end up in databases of EISA, are secured to the highest level and with the state of the art technology.

On the other hand, secrecy is necessary in cybersecurity. Reasonable level of secrecy helps to ensure security – not everyone must know every detail. Just like with national security, cybersecurity needs discretion, confidentiality and reasonable level of secrecy. Estonian draft for Cybersecurity Act walk on the sharp edge of being opaque, but for every point where there is lack of transparency, secrecy can be justified.

It is understandable that there will never be eternal transparency, secrecy in some cases is extremely necessary. Such cases might involve information about national security strategies and information about secret services. Unfortunately, it is the author's opinion that the new Cybersecurity Act does not balance transparency and secrecy to its best. Too many issues are left unresolved and many questions arise from reading the draft regulation.

On the other hand, the new draft law makes a great effort to harmonize definitions and to seek clear descriptions on who will be understood to be the subjects of the new law. This is great effort from the legislators, since thus far Estonia has not had unified language use.

5. CONCLUSION

To conclude, throughout the years the European Union has shown growing interest in ensuring safe cyberspace for all. There have been many initiatives such as the GDPR, ePrivacy Regulation and NIS Directive.

The NIS Directive aims to achieve high common level of cybersecurity throughout the European Union. Unfortunately, the Union legislators decided to opt for more of soft legislation in a sense that they decided to regulate cybersecurity with a directive rather than a regulation. The European Union will see if this measure is enough or maybe there will be new additional legislations implemented and the new directive overturned.

In conclusion, the new draft law to implement the European Union NIS Directive certainly lacks transparency in some parts. The legislators in Estonia have tried to cram as little as possible into a very short regulation. Cybersecurity is an important aspect of our society and it is the author's opinion that much greater job could have been achieved.

This thesis tried to answer two main questions, which were

1. What are the legal obstacles that prevent the application of transparency norms in relation to NIS implementation in Estonia?

2. Does the implementing law strike fair balance between secrecy and transparency?

It is the author's opinion that Cybersecurity Act gravitates towards non-transparent regulation. For example, many important aspects about EISA's operations have been left out, such as remedies in case of over stepping boundaries or what even are the boundaries under the Cybersecurity Act.

It is the author's opinion the new Cybersecurity Act does not really strike a fair balance between transparency and secrecy. Too many aspects, which would need transparency are left

under a cloak of secrecy. In the author's opinion that this secrecy is not strived to on purpose, rather the Estonian draft composers have tried to cram whole cybersecurity related regulation into a fairly short draft and have not really aimed for the most transparent and clear regulation, and therefore Estonia will end up with non-transparent piece of legislation which will govern national network and information systems security.

But then again, it is widely known that transposing and implementing every piece of European Union legislation to a perfection is difficult, if not impossible. There are many pieces of legislation which need to be implemented in a fairly short amount of time, so some directives and regulations may not be transposed to a perfection but thankfully Estonia can substitute and correct this new upcoming law in the future if it deems necessary.

There are many legal obstacles that prevent the application of transparency norms, some of these obstacles come from regulations which concern private entities. For example, under the Competition Act it is unlawful to publicize business secrets, but with the new Cybersecurity Act it will become an issue. Log data must be classified, and regular people might never know what kind of cyber incident took place or whether it affected him/her.

In addition to legal obstacles, there is an issue of novelty of network and information systems security. Most of the legislators are strangers to the information technology side of issue at hand. Many if not most of legislators lack knowledge, which makes a perfect storm for legislation which is overreaching, under regulating or lacking real-life applicability in real situations which occur.

This thesis also gave the reader an overview of the NIS Directive and overall cyber related legislation that has come out or is on its way to approval in the European Union.

At the time of concluding this thesis paper, the new Cybersecurity Act has been entered into accepted and sent for overview for the Estonian President. The most honest and real review of the new draft legislation can be made after it takes effect.

Once the new law is in force the actual issues of applicability will start to arise and only then one could clearly say whether the new legislation strikes a fair balance between transparency and secrecy. In case there will be many issues one can assume that there has been left too-too many uncertainties and unanswered questions. In case where every subject of this new legislation will understand its responsibilities, duties and rights the new draft has been successful in ensuring transparency.

Estonia did a fair job with the NIS Directive implementation. As with any legislation there could be more clarity, fairness and governmental responsibility implied. Regardless, it is difficult to give definitive assessment before the new legislation is in force.

6. LIST OF REFERENCES

6.1. Books

1. Craig, P., de Burca, G. (2015). *EU Law: Text, Cases, and Materials.* 6th edition, 1-1159. Oxford University Press.

6.2. Articles

2. van Aaken, A., Wildhaber, I. (2015). State Liability and Critical Infrastructure: A Comperative and Functional Analysis. – *European Journal on Risk Regulation,* Vol. 2 (2015), 244-254. HeinOnline.

3. Barnard-Wills, D. (2013). Security, privacy and surveillance in European policy documents. – *International data Privacy Law,* Vol. 3, No. 3, 170-180. Oxford University Press.

4. Bradley, C., M. (2012). Transparency and Financial Regulation in European Union: Crisis and Complexity. – *Fordham International Law Journal,* Vol. 35:117, 1171-1206. HeinOnline.

5. Bertot, J. C., Jaeger, P. T., Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social meida as openness and anti-corruption tools for societies. – *Government Information Quarterly,* Vol. 27, 264-271. Elsevier Ltd.

6. Birchall, C. (2012). The Politics of Opacity and Openness. Intorduction to Transparency. – *Theory, Cluture & Society,* Vol. 28, Issue 7-8, 1-19. SAGE Publications.

7. Burden, K. (2016). European Union Update. – *Computer Law & Security Review,* Vol. 32, 363-368. Elsevier Ltd.

8. Burden, K. (2015). European Union Update. – *Computer Secuirty & Law,* Vol. 31. 810-815. Elsevier Ltd.

9. Cormack, A. (2016). Incident Response: Protecting Individual Rights Under the General Data Proetction Regulation. – *A Journal of Law, Technology & Society,* Vol. 13, Issue 3, 259-282. Script*ed.*

10. Denyer, D., Kutsch, E., Lee-Kelley, E., Hall, M. (2011). Exploring reliability in information systems programmes. – *International Journal of Project Management,* Vol. 29, 442-454. Elsevier Ltd.

11. Dimitrakopoulos, D.G. (2001). The Transposition of EU Law: 'Post-Decisional Politics' and Institutional Autonomy. – *European Law Journal,* Vol. 7, number 4, 442-458. Blackwell Publishing Ltd.

12. Esayas, S. (2014). Breach Notification Requirements Under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance. – *The John Marshall Journal of Information Technology & Privacy Law,* Vol. 31, Issue 3, Article 2, 317-368. The John Marshall Institutional Repository.

13. Fang, F., Parameswaran, M., Zhao, X., Whinston, A.B. (2014). An economic mechanism to manage operational security risks for inter-organizational information systems. – *Information Systems Frontiers,* Vol. 16, Issue 3, 399-416. Springer Science + Business Media, LLC.

14. Fahey, E. (2014). The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security. – *European Journal of Risk Regulation,* Vol. 5, Issue 1, 46-60. HeinOnline.

15. Holzleitner, M.-T., Reichl, J. (2017). European provisions for cyber security in smart grid – an overview of the NIS-directive. – *Elektrotechnik & Informationstechnik,* Vol. 134, No. 1, 14-18. Germany: Springer Verlag Wien.

16. Janssen, M., Charablabidis, Y., Zuiderwijk. (2012). Benefits, Adoption Barriers and Myths of Open Data and Open Government. – *Information Systems Management,* Vol. 29, No. 4, 258-268. Taylor & Francis Group.

17. Hwang, K., Choi, M. (2017). Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism. – *Government Information Quarterly,* Vol. 34, 183-198. Elsevier Ltd.

18. Hojnik, J. (2016). The servitization of Industry: EU law implementations and challenges. – *Common Market Law Review,* Vol. 53, Issue 6, p.1575-1623. The Netherlands: Wolters Kluwer Law and Business.

19. Kelli, A. (2015). The conceptual bases for codifying Estonia's IP law and the main legislative changes: From the comparative approach to embedding drafted law into socio-economic conext. – *International Comparative Jurisprudence,* Vol. 1 (2015), 44-54. Elsevier Ltd.

20. Kreutz, D., Malichevskyy, O., Feitosa, E., Cunha, H., da Roda Righi, R., de Macedo, D. D.J. (2016). A cyber-resilient architecture for critical security services. – *Journal of Network and Computer Applications,* Vol. 63, 173-189. Elsevier Ltd.

21. Lafarge, F. (2010). Administrative Cooperation between Member States and Implementation of EU law. - *European Public Law,* Vol. 16, No. 4, 597-618. HeinOnline.

22. Laube, S., Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. – *Journal of Cybersecurity,* Vol. 2, Issue 1, 29-41. Oxford University Press.

23. Luiijf, E., Besseling, K. (2013). Nineteen national cyber security strategies. – *International Journal of Critical Infrastructures,* Vol. 9, No. ½, 3-31. The Netherlands: Inderscience Enterprises Ltd.

24. Manley, M. (2015). Cyberspace's Dynamic Duo: Forgning a Cybersecurity Public-Private Partnership. – *Journal of Strategic Security,* Vol. 8, No. 5, Article 9, 85-98. Henley-Putnam University Press.

25. Maxeiner, J. (2007). Legal Certainty and Legal Methods: A European Aletrnative to American Legal Interminancy? – *Tulane Law School of International Law & Comperative Law,* Vol. 15, 541-607. HeinOnline.

26. Papaloi, A., Gouscos, D. (2013). Parliamentary Information Visualization as a Means for Legislative Transparency and Citizen Empowerment? – *eJournal of eDemocracy & Open Government,* Vol. 5, No. 2, 174-186. Academic Conferences and Publishing International Limited.

27. Peters, A. (2010). Transparency, Secrecy, and Security: Liaisons Dangereuses. – *Rule of Law, Freedom, and Security in Europe,* Vol. 6, 183-243. Europe, Brussels: Bruylant.

28. Posen, B. R. (2006). European Union Security and Defence Policy: Response to Unipolarity? – *Security Studies,* Vol. 15, No. 2, 149-186. Taylor & Francis Group.

29. Raab, C., Szekely, I. (2017). Data protection authorities and information technology. – *Computer Law & Security Review,* Vol. 33, Issue 4, 421-433. Elsevier Ltd.

30. Relly, J. E., Sabharwal, M. (2009). Perceptions of transparency of government policymaking: A cross-national study. – *Government Information Quarterly,* Vol. 26, 148-157. Elsevier Ltd.

31. Sales, N. A. (2013). Regulating Cyber Security. – *Northwestern University Law Review,* Vol. 107, No. 4, 1503-1568. HeinOnline.

32. Scheau, M.-C. (2017). Strategic Management of Critical Infrastructures and Financial Domain. – *International Journal of Information Security and Cybercrime,* Vol. 6, Issue 1/2017, 13-24. HeinOnline.

33. Shore, J. J. M. (2015). An Obligation to Act: Holding Government Accaountable for Critical Infrastructure Cyber Security. – *International Journal of Intelligence and CounterIntelligence,* Vol. 28, Issue 2, 236-251. Taylor & Francis Group.

34. e Silva, K. (2013). Europe's Fragmented Approach Towards Cyber Security. - *Internet Policy Review,* Volume 2, Issue 4, 1-8. Germany: Alexander von Humboldt Institute for Internet and Society.

35. Sliwinski, K. R. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent. – *Contemporary Security Policy,* Vol. 35, No. 3, 468-486. Taylor & Francis Group.

36. van der Sloot, B. (2015). Do privacy and data protection rules apply to legal persons and should they? A proposal for two-tier system. – *Computer Law & Security Review,* Vol. 31, Issue 1, 26-45. Elsevier Ltd.

37. Sullivan, C., Burger, E. (2017). E-residency and blockchain. – *Computer Law & Secuirty Review,* Vol. 33, 470-481. Elsevier Ltd.

38. Timmermans, C. (1998). Subsidiarity and Transparency. – *Fordham International Law Review,* Vol. 22, Issue 6, Article 8, 106-126. United States: Fordham University School of Law.

39. Vlaicu, A.-M. (2011). Effectivness of EU law in member states. – *Lex ET Scientia International Journal,* Vol. 18, Issue 1, 162-173. HeinOnline.

40. Voermans, W., ten Napel, H.-M., Passchier, R. (2015). Combining efficiency and transparency in legislative process. – *The Theory and Practice of Legislation,* Vol. 3, Issue, 3, 279-294. Taylor & Francis Group.

41. Webber, M., Taylor, S. (2016). The NIS Directive – a practical perspective. – *Privacy & Data Protection,* Vol. 16, Issue 3, 9-12. Westlaw, Thomson Reuters.

42. Wenander, H. (2013). A Network of Social Security Bodies – European Administrative Cooperation under Regulation (EC) No 883/2004. – *Review of European Administrative Law,* Vol. 16, No. 1, 39-71. Paris Legal Publishers.

6.3. European Union legislation

43. The European Parliament and the Council of the European Union (EU) No 2016/1148 of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union, OJ L 194/1, 19.07.2016.

44. The European Parliament and the Council of the European Union (EU) No 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 04.04.2016.

45. European Commission Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union COM(2013) 48 final of 7.2.2013.

46. European Commission Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions JOIN(2013) 1 final of 7.2.2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure cyberspace.

47. European Commission Joint Communication to the European Parliamnet, the Council JOIN(2017) 450 final 13.9.2017 Resilience, Deterrance and Defence: Building strong cybersecurity for the EU.

48. Communication to the European Parliament, the Coucil COM(2010) 673 final of 22.11.2010 The EU Internal Security Startegy in Action: Five steps towards a more secure Europe.

49. European Commission. Proposal for a Regulation on Privacy and Electronic Communications COM(2017) 10 final of 10.1.2017

6.4. Estonian national legislation

50. Avaliku teabe seadus, RT I, 04.07.2017, 11.

51. Eesti Vabariigi Põhiseadus, RT I, 15.05.2015, 2.

52. E-identimise ja e-tehingute usaldusteenuste seadus, RT I, 25.10.2016, 1.

53. Elektroonilise side seadus, RT I, 01.07.2017, 2

54. Hea õigusloome ja normitehnika eeskiri. RT I, 29.12.2011, 228.

55. Hädaolukorra seadus, RT I, 28.12.2017, 49.

56. Infosüsteemide turvameetmete süsteem, RT I, 2007, 71, 440.

57. Isikut tõendavate dokumentide seadus, RT I, 21.04.2018, 5

58. Konkurentisseadus, RT I 20.12.2017, 7

59. Küberturvalisuse seadus, Eelnõu.

60. Lennundundusseadus, RT I, 03.03.2017, 16.

61. Raudteeseadus, RT I, 16.05.2017, 3.

62. Riigi Infosüsteemi Ameti põhimäärus, RT I, 28.04.2011, 1

63. Riigikaitse seadus, RT I, 27.06.2017, 6

64. Riigisaladuse ja salastatud välisteabe seadus, RT I, 05.05.2017, 5

65. Sadamaseadus, RT I, 03.03.2017, 24

66. Töölepingu seadus, RT I, 28.12.2017, 43

6.5. Electronic sources

67. Majandus- ja Kommunicatsiooniministeerium. (2017). *Küberturvalisuse seaduse eelnõu seletsukiri.* Accessible from: http://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b#90L0yx37. Last accessed on: 06.03.2018.

68. Majandus- ja Kommunicatsiooniministeerium. (2017). *Küberturvalisuse seaduse eelnõu.*. Accessible from: http://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b#90L0yx37. Last accessed on: 06.03.2018.

69. Männiko, M., Maaten, E., Poola, M., Männiko, M., Kinkar, R., Rull, A. (2016). *Kübervaldkonna õigusanalüüs.*Accessible: https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf. Last accessed: 06.03.2018.

70. Majandus ja Kommunikatsiooniministeerium. *Kübervaldkonna seaduse väljatöötamise kavatsus.*Accessible from: http://eelnoud.valitsus.ee/main/mount/docList/3529d47c-0b7c-4f39-9003-4a839a7d8c49#goFNzNsW, 09.03.2017. Last accessed: 06.03.2018.

71. Majandus- ja Kommunikatsiooniministeerium. (2017). Küberturvalisuse seaduse eelnõu, legislative draft number 17-1087. – [E-database] http://eelnoud.valitsus.ee/main/mount/docList/775b7e36-09e2-480f-9217-81fb79ed293b#L1XT55BW. Last accessed:17.02.2018.

72. Riigikontroll. (2014). Ülevaade riigi varade kasutamisest ja säilitamisest 2013-2014. aasta. [Online] http://www.riigikontroll.ee/Riigikontrollipublikatsioonid/Riigikontrolliaastaaruanneparlamendile/tabid/110/ItemId/434/View/Docs/amid/732/language/et-EE/Default.aspx. Last accessed: 07.03.2018.

73. Kahu, O. (2017). Pärnu maanteele tulevad elektroonsed liiklusmärgid. – *Eesti Rahvus Rimghääling,* 15. May. Accessible from: https://www.err.ee/595994/parnu-maanteele-tulevad-elektroonilised-liiklusmargid. Last accessed: 05.03.2018.

74. ENISA. ENISA overview of cybersecurity and related terminology. Version 1, September 2017. Accessible: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology. Last accessed on: 02.02.2018.

6.6. Other sources

75. Turcu, D. (2016). Considerations on cyber security legislation and regulations in Romania.- *International Scientific Conference ''Strategies XXI'',* Bucharest. Bucharest: National Defence University, 173-180.