HELSINGIN YLIOPISTO

EU Cybersecurity and Media Companies: Impact of the NIS2 Directive

Oikeustieteen maisterin koulutusohjelma
Maisterintutkielma
Tekoälyoikeuden projektiseminaari: Tekoälyn yhteiskunnallis-oikeudelliset vaikutukset

Author:
Lauri Halonen

Supervisors:
Docent Suvi Sankari
Associate Professor Riikka Koulu

12.11.2024
Helsinki

Faculty: Faculty of Law

Degree programme: Oikeustieteen maisterin koulutusohjelma (Master of Laws)

Study track: European law

Author: Lauri Halonen

Title: EU Cybersecurity and Media Companies: Impact of the NIS2 Directive

Type of work: Master's thesis

Month and year: November 2024

Number of pages: iv + 85

Keywords: cybersecurity, NIS2 Directive, media companies, European Union, risk-management, public broadcasting, critical entity, security of supply

Supervisors: Suvi Sankari, Riikka Koulu

Location: Helsinki University Library

Additional information:

Abstract:

The importance of cybersecurity for entities in the European Union is in a growing phase. The change in the security situation in Europe is closely connected to the increase of cybersecurity threats in Europe, which have become more prevalent in the last few years. Digital transformation has fundamentally changed the way organisations across all sectors operate, increasing both their reliance on technology and exposure to cyber risks. This also applies to media companies.

The European Union proposed the NIS2 Directive in 2020, which repeals the original NIS Directive. NIS2 aims to obligate critical entities to implement adequate cybersecurity measures in order to achieve a high common level of cybersecurity across the European Union. The question of whether or not the NIS2 imposes rules on media companies is not simple, as media companies are not explicitly mentioned anywhere in the Directive text. This thesis uses legal doctrinal analysis as the research method.

The goal of this thesis is to find out if media companies are in the scope of NIS2, and to assess the impact of the Directive on media companies in the Union area, and to provide operational recommendations for these organisations on implementing the actual risk-management measures following the implementation of the NIS2. This thesis also discusses and provides insight on the developments of EU cybersecurity regulation and discusses its necessity for the overall security in the Union. This thesis was commissioned by Yleisradio Oy, the Finnish Broadcasting Company.

After the introduction, in its second chapter, this thesis discusses the European Union's Cybersecurity Strategy and current operational environment of media companies in the Union area, and defines the entity type this thesis is focused on and has a brief introduction to cybersecurity and different types of cyber threats.

The third chapter focuses on the NIS2 Directive. It explains the origins of the Directive, and what the Directive aims to achieve. It also explains the scope of the Directive and analyses the possibility of its applicability to media companies, concluding that media companies which own the network they use and some of the European public broadcasting companies could well be regarded as falling within the scope of the Directive by the wording of the Directive and consequently the national laws following the implementation of the Directive. The fourth chapter introduces the CER Directive into the analysis, which is to be implemented and complied with in close coordination with the NIS2 Directive. It also has an impact on the scope of application of the NIS2. The chapter completes the analysis by

examining other contextual factors that affect the scope of the NIS2, and briefly reviews national implementation decisions taken by a few Member States that have an effect on public broadcasting companies. The chapter concludes that public broadcasting companies may fall within the scope of the Directive if their specific characteristics meet the definition of public administration for the purposes of the Directive.

The fifth chapter discusses the cybersecurity risk-management measures the NIS2 Directive requires of entities in the scope of application of the Directive, with the sixth chapter reviewing and adding to the critique towards the NIS2, providing insight on the predicted effectiveness and necessity of the Directive as a legislative instrument for the development of cybersecurity in the European Union. The seventh chapter provides operational recommendations and best practices for media companies on reacting to the new Directive, both in the cases of whether or not they fall within the scope of application of the Directive. The eighth chapter concludes and expresses the limitations of the study, along with the closing words of the author.

Table of contents

1 Introduction

1.1 Short overview of the topic

The security situation in the European Union is in transition. Russian Federation's brutal invasion of Ukraine shook the Europeans' perception of their own security and raised the likeliness of a war in Europe in the minds of Europeans. Instabilities in Middle East concern Europe and geopolitics between the US, China and Russia have Europe in a challenging position as a middleman. Attitudes and relations towards these large players vary between European countries and even between the European Union Member States.

This change in the security situation in Europe is closely linked to the increase in cyber security threats in Europe, which have become more prevalent in the last few years. In addition to the obvious cyber-attacks on Ukraine, Russian (among others) organisations conduct attacks on other European nations, and this has raised the question of the actual robustness and level of cyber security resilience in the European Union.[1] Even before Russia's invasion of Ukraine in 2022, cybersecurity was a major risk, with an estimated ransomware attack occurring globally every 11 seconds in 2021.[2] This is estimated to drop to every 2 seconds in 2031.[3] Ransomware attacks have been used to jeopardise the functioning of entire governments, as was the case with the Bundestag attack in 2015,[4] and again in 2021,[5] and in a minor attack on Finland's parliament in 2020,[6] and on several ministries in 2022.[7] These are just a drop in the ocean of cyberattacks on European nations and organisations, but they show that attacks can cripple the functioning of entire governments, and attacks like these are a useful tool for nations in times of war, or when a disruption or external influence is needed for any reason.

---

[1] Bassot, 'Ten Issues to Watch in 2023."
[2] Morgan, "2022 Cybersecurity Almanac."
[3] Morgan "Global Ransomware Damage."
[4] Cerulus, "EU Sanctions Russian Hackers."
[5] Der Spiegel, "Russische Gruppe »Ghostwriter« attackiert offenbar Parlamentarier."
[6] Eduskunta, "Eduskuntaan on kohdistunut kyberhyökkäys."
[7] Valtioneuvosto, Statsrådet (@valtioneuvosto), "Valtioneuvoston ja ministeriöiden verkkosivustoihin kohdistuu tällä hetkellä palvelunestohyökkäys."

The world of 2024 is very different from the world we lived in, say, in 2000. The services we consider essential are very different from those we considered essential 24 years ago. We are now more dependent on electronic services, which have different vulnerabilities from the services we used to depend on. The food on the supermarket shelves and the connections and relationships with other people in people's lives today depend on technology. We have become accustomed to today's technology, and we do not fully understand how these technologies work or what their vulnerabilities are. In order to function correctly, these technologies need infrastructure that is resilient to cyberthreats. This means that the essential services have to be able to protect themselves, and to continue functioning in an event of a crisis or other incident that threatens the functioning of said service.[8]

The European Union has been active in developing its own cybersecurity framework and is committed to helping Member States and European organisations develop effective cybersecurity measures. Advances in cyber-attack techniques, the increase in their prevalence and, consequently, in the damage they cause, justify a review of the legislation. This development focuses in particular on entities that are considered critical by Member States. The Directive (EU) 2022/2555,[9] hereafter NIS2, is an important part of this development.

Digital transformation has fundamentally changed the way organisations across all sectors operate, increasing both their reliance on technology and exposure to cyber threats. The role of the media is crucial in ensuring that information continues to reach the public. If a generally relatively trustworthy media company does not have adequate security measures in place, society could fall into a kind of news blackout in a time of crisis, and people would not have access to reliable sources of news and information. This makes media companies, in principle, a highly critical sector. Media companies can also be important actors in the distribution of public emergency warnings, as they can, and in some cases are required or expected to

---

[8] Calder, Network and Information Systems (NIS) Regulations - a Pocket Guide for Operators of Essential Services, 7-10.

[9] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).

broadcast warnings nationally on radio and television channels.[10] The application of the NIS2 Directive to media companies is not clear from the text of the Directive alone. Media companies are not mentioned anywhere in the Directive. It is therefore not clear whether the Directive applies to such companies.

1.2 Scope of the thesis

This thesis will focus mainly on Union legislation and will not be an exhaustive study of the national implementation measures. National legislation will be examined to look at differences in implementation and interpretation between Member States.

This thesis was commissioned by Yleisradio Oy (Yle), the Finnish Broadcasting Company. The objective was to assist Yle in determining whether the NIS2 Directive applies to the company. The aim was also to enable other European media companies to benefit from the thesis. This is why the thesis was written in English, with a Europe-wide focus, and not focusing only on the measures to be taken by Yleisradio Oy. Due to the focus on Union legislation, it should be noted that this thesis does not seek to provide a definite or conclusive answer to the question of what national legislation will require from any individual media company. The assessment must be carried out on an individual basis, as the specific characteristics of companies vary greatly, and affect the assessment.

1.3 Research methods and material

1.3.1 Scientific research

Scientific research aims to find answers and to provide explanations and insights into various phenomena.[11] Research should have a critical and analytical perspective and

[10] In Finland, emergency notifications are broadcast on Yle and MTV3, all radio stations, text TV, and through a mobile application. They are also shown during programmes. Read more at https://www.suomi.fi/citizen/rights-and-obligations/security-and-public-order/guide/what-to-do-in-an-emergency/alerting-the-public.
[11] Keinänen and Väätänen, ”Empiirinen oikeustutkimus – mitä ja milloin?,” 246.

be open-minded to different points of view. This is seen as the main goal of academic work in Finnish legal scholarship,[12] and I intend to uphold this objective.

In scientific research, it would be beneficial for the success of the research to identify the exact field of research in the discipline in which the work is being written. This thesis has been written as part of the artificial intelligence law seminar project. AI is increasingly relevant to cybersecurity, but it is certainly not yet in the core of day-to-day cybersecurity measures implemented by companies.[13] This thesis departs from more obvious AI law topics and has its place in the field of European Union law, including aspects of information security law, and regulatory compliance. This is because the thesis focuses on the NIS2 Directive, an EU secondary legislation instrument, with considerations on the actual cybersecurity measures to be implemented in organisations. The proximity of technology law and the potential use of AI in cybersecurity relate the topic of the thesis reasonably well to the general theme of the project seminar, which is the socio-legal implications of AI.

1.3.2 Research methods

Legal research can be conducted using a variety of research methods. Defining a single method to be used in legal research is not easy or simple, nor is it usually done in a sustained or robust way.[14] It also seems that there is no single way in which legal scholars view or agree on the nature of the methods of legal research,[15] nor is there a single correct way to analyse the legal doctrine.[16] These discussions do not make it easy to define the methodology for this thesis. In the author's view, the method of this thesis can best be described as legal doctrinal analysis, as the main goal of this thesis is to analyse the scope of application of the NIS2 Directive and its possible application on media companies.

Legal doctrinal analysis as a research method is not seen in the same way everywhere, which is not a surprise considering the differences in legal systems between the

---

[12] Sajama, ”Mikä tekee tutkimuksesta tieteellisen?,” 16–18.
[13] There are some applications of AI used in cybersecurity, but it is not yet widespread, as it still is problematic regarding matters such as false alarms, privacy and trade secrets. AI could also be used for creating cyber threats, which is a huge risk for organisations affected but also the developers of the AI models. This will most probably change in the future, as technology progresses.
[14] Hirvonen, *Mitkä metodit?: opas oikeustieteen metodologiaan,* 7.
[15] Hoecke, Mark Van. "Legal Doctrine: Which Method(s) for What Kind of Discipline?." 17.
[16] Kangas, “Minun metodini,” 91.

Anglo-American world and European countries,[17] and the apparent ambiguity of the methodology of legal research.

Legal doctrinal analysis is structured around analysing legal acts, specific articles, the act's preliminaries, preambles or history of the act, and the analysis of specific cases that constitute case law. The purpose of legal doctrinal analysis is to provide answers on how legal texts should be interpreted.[18] These interpretations are what ultimately constitute the actual legal doctrine. Legal interpretation can be conducted by several different methods. The goal of interpretation of legal texts in a specific legal question or case is to arrive from factual description to a statement of interpretation.[19] This seems quite pragmatic, and the reality here is that this thesis can be seen as having somewhat of a practical character, which is one of the main characteristics of the legal doctrinal analysis method,[20] and it can be rightfully questioned if there is any difference between practical action and the legal doctrinal analysis method.[21] It has been argued that much of the apparently scientific research in the field of law, at least in Finland, would not pass the "test" of scientific research.[22] This thesis mainly aims to provide a pragmatic answer to the question of whether or not companies are in the scope of the NIS2 Directive and if they have any obligations under the new Directive, and to explain those obligations. This is fundamentally a business compliance issue, integral to the compliance and risk management responsibilities of organisations.

Legal doctrinal analysis has as its objective the explaining of exact meaning behind legal texts and norms. It is inherently a science of giving justified interpretations.[23] These legal norms may refer to expressions of legal language, content of said legal expressions, or a combination of both. Any take on what a legal norm really says is inherently an interpretation of legal norms. The legal norms described here have to be understood broadly, including rules such as national law, acts, regulation, and cases, and on top of these, supra-, transnational and international legislation and

---

[17] Van Gestel and Micklitz, *Revitalizing Doctrinal Legal Research in Europe: What About Methodology?* 26.
[18] Rautiainen, Kostiainen, Kurki, Soininen, and Määttä, *Oikeus ja sen tutkiminen*, chapter 3.
[19] Hirvonen, *Mitkä metodit?: opas oikeustieteen metodologiaan,* 38.
[20] Aarnio, "Oikeussäännösten systematisointi ja tulkinta," 48. Aarnio argues that instead of asking if legal doctrinal analysis or legal dogmatics *is science,* one should ask what it is in practice in day-to-day research work.
[21] Aarnio, *Essays on the Doctrinal Study of Law*. 19.
[22] Mäntysaari, "Onko Legal Design tiede? Havaintoja erään väitöskirjan perusteella," 187–188.
[23] Hirvonen, *Mitkä metodit?: opas oikeustieteen metodologiaan,* 36.

case law, such as rulings of the Court of Justice of the European Union (CJEU), and any work papers given on or during drafting or preparing the legislation.[24] The material that influences the interpretation can therefore be quite extensive, and all of it helps the interpreter to reach his or her conclusions.

In my analysis, I aim to provide a broader view of the European cybersecurity landscape and clarify the intended achievements of the NIS2 Directive within this legislative context. I seek to contribute to the discourse on European cybersecurity law and its development, analysing the necessity and effectiveness of the NIS2 Directive as a legal instrument. This approach aligns with the methodology chosen here. The incorporation of a position statement that includes both *de lege lata* and *de lege ferenda* analyses are beneficial and consistent with legal doctrinal analysis.

1.3.3 Legal interpretation

Legal terms and natural language are not interpreted universally in the same way. Lawyers can and do have different methods to interpreting legal texts. These can be utilized in different ways in different situations and, for example, in promoting a client's situation to a desired direction. Some of these are intertwined and some are used more frequently than others. It is important to be able to identify and name the method used when interpreting legal texts, in order to really understand the effect of one's own preferences, political views and prejudices. In this way, the interpreter has legitimate confidence and competence in interpreting the legal text, whatever the purpose of the interpretation or possible bias. Legal interpretation methods should be used in conjunction with each other in order for the interpretation to be complete, but in the other hand, exclusion of a certain interpretation method does not render the interpretation erroneous or inaccurate.[25]

A (post)modern approach, on methods of legal text interpretation, and one that this thesis will aim for, has been explained by Seppo Sajama, who looks at legal interpretation as a funnel, or as Sajama puts it, a "shooting star," with three alternative trails, each stemming from a single main method of interpretation. This approach offers an excellent, yet simple descriptive description of the cognitive

---

[24] Ibid, 23.
[25] Savigny, System Des Heutigen Römischen Rechts, 215.

processes that a lawyer should adopt, at least within the European context of legal academia. However, it must be kept in mind that this is largely the method students are taught in Finnish universities and therefore familiar also to the author of this thesis. Other approaches to the methods of interpretation have been also identified, that are not in any way inferior to the one explained by Sajama.[26]

The methodical road map pictured by Sajama is as follows; A) zero-context as the main and first approach if there absolutely is no contextual information that could provide deviations to the textual interpretation. If and when there is reasoning for other interpretations, we have the B) Psychological context; intentions of the legislature, C) Textual context; possible conflicts between internal or external legal texts and the legislation text, and D) Outer context; advantages and disadvantages of different interpretations and their consequences. The alternatives B, D, and C are all equal and have no priority over the other. In reality, there is never a pure non-contextual interpretation of any legal text, as thorough legal interpretation will always require assessing at the other three options.[27] It is inevitable that a degree of interpretation will occur when a human being is interpreting legislation, as past experiences and knowledge inevitably influence the assessment.

A legal researcher should know which interpretation methods to use in which cases. In this thesis the focus is on law of the European Union, and it has to be interpreted accordingly. In EU law, only text that is considered highly ambiguous or confusing can be interpreted as deviating from the usual meaning of words.[28] Language differences and translations of EU legislation can also affect interpretations, although all language versions are equally authentic.[29] This makes the interpretation of EU legislation a difficult task, as all language versions have to, at least theoretically, be given equal consideration. EU law is interpreted more or less in the same way as national or international legislation, i.e. using the same interpretation methods. However, in interpreting EU legislation, systematic and teleological interpretation

---

[26] See Hirvonen, Mitkä metodit?: opas oikeustieteen metodologiaan, 38–40 for a list of interpretation methods Hirvonen has identified.
[27] Sajama.”Argumentaatio Oikeustieteellisessä Tutkimuksessa.” 34–35.
[28] Lenaerts and Gutiérrez-Fons, “To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice”, 7.
[29] Case 283/81 CILFIT, par. 18 confirmed that all language versions of directives are equally authentic. Additionally, Article 55 Treaty on European Union, and Article 358 Treaty on the Functioning of the European Union set the primary language rules on EU law.

methods have historically had a strong stance.[30] In systematic interpretation, other legal rules, principles, theories and the legal system as a whole are considered, and in teleological approach, the objective of the regulation, and consequences of different interpretation options are identified, and the interpretation that best contributes to the legislators' objective is chosen. This is because of the language used in EU treaties and their usual perceived vagueness.[31] It can be said that the treaties are often drafted in a broad manner by design, as their goal is to establish EU law principles rather than to define the precise meaning of a particular expression.[32] In today's, and in more sector-specific legislation, the EU legislator has used a more nuanced language to reduce ambiguity. This is true for example in newer EU directives, where the language used is remarkably clear and precise.[33] In the context of this study, this argument appears somewhat simplistic, given that there are often multiple interpretations of the wording of texts. A person interpreting law should not steer away from the literal wording of the text if there is no reason for it.[34] It is justified to rely on the literal content of the text that the legislature has written. If there is no possibility of any other interpretation, the rule must be interpreted strictly in accordance with its wording. This means that the other interpretations have to be examined before an interpreter can come to any conclusion.[35]

In examining the applicability of the Directive on media companies, this thesis begins with an analysis of the literal wording of the legislation. Then I will have a look at other interpretations but will keep in mind that the literal wording of the legislation text is the most authoritative one. Furthermore, I will examine national implementation measures that have been put in place by a few EU Member States following the NIS2. It is important to note that this does not constitute comparative legal research in terms of methodology, nor does it seek to present itself as such.

---

[30] Ojanen, EU-Oikeuden Perusteita, 51-52. Also Hirvonen, "Mitkä metodit?: opas oikeustieteen metodologiaan", 40.
[31] Ibid, 52.
[32] Lenaerts and Gutiérrez-Fons, "To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice", 13.
[33] Ojanen, EU-Oikeuden Perusteita, 52.
[34] Hirvonen, Mitkä metodit?: opas oikeustieteen metodologiaan, 32.
[35] Sajama, "Argumentaatio Oikeustieteellisessä Tutkimuksessa," 34–35.

1.3.4 Research material

Research material used in this thesis includes legislature and relevant legal and information-technological literature, scientific papers on cybersecurity and other security-related literature in the context of the EU and on media companies in the Union region. Legislature includes European Union level legislation and national legislation, and literature includes works done in and outside of the Union, primarily in Finnish and English.

1.4 Research questions

The main research question of the thesis is: Do media companies fall under the scope of the NIS2 Directive? Answering this question leads to the supplementary research question of this thesis: What is the impact of the Directive on media companies operating within the Union? This question focuses on the actual measures that companies would have to take if they are within the scope of the Directive.

This thesis also discusses and provides insight on the developments of EU cybersecurity regulation and discusses its necessity for the overall security in the Union and so contributes to broader academic discussions on the European cybersecurity legislative developments and the role of media companies for our societies.

In order to answer to the main research question, it is essential to assess the scope of application of the Directive and the possibility of inclusion of media companies within its scope. This question of applicability of the NIS2 Directive is by its nature quite a novel subject, as the Directive is fairly recent. However, there is some research that has been conducted on and around this subject. In fact, legal literature has been written on the scope of application of the Directive. Yleisradio Oy has also earlier ordered a case study which touched on this question, but the previous study took a more practical approach, focusing on recommendations for action rather than a legal doctrinal analysis of the scope of application of the Directive.[36] Scope of application

[36] The study was not intended to be a legal study.

of the NIS2 nor the Directive (EU) 2022/2557, hereafter CER Directive,[37] on media companies was not extensively analysed. This was correctly recognised by the author.[38]

Research has been conducted on the necessity and feasibility of the Directive, which will be referenced to and provided a take on. This will target the supplementary research question of real-world impact of the Directive on media companies. This research area has focused on the additions the NIS2 Directive brings to the regulation scheme by replacing the original NIS Directive (hereafter NIS1).[39] Research has also been carried out on the specific reporting obligations, with a focus on better defining the obligations.

All in all, it seems like the Directive has been studied thoroughly when taking into account the research done on the first NIS Directive and research done in the limited time the proposal for the NIS2 has been available. Research has not been conducted in the exact scope of this thesis. This could well be because these companies are not very obviously in the core target group of cybersecurity legislation. These companies could still benefit from this thesis and its recommendations. This thesis could also have a part in driving a more connected cybersecurity co-operation between European media companies.

Based on earlier research on the scope of application and on the nature of the NIS2 Directive and its aim, including the preamble text, my hypothesis for this thesis is that media companies are not in the scope of the Directive, at least by default. This conclusion is based on the fact that media companies are not explicitly mentioned anywhere in the Directive, and previous research has not identified them as falling within its scope. It is clear that media companies are not as critical as for example entities in infrastructure sectors such as energy, transport or financial markets infrastructure. The core function of media companies is not as critical as of those, and therefore it has to be assumed that media companies would be left out of the scope of the Directive. However, the individual characteristics of certain media companies

---

[37] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
[38] Lilja, “CER- ja NIS2-direktiiviehdotusten vaikutus mediayhtiön varautumiseen: Case Yleisradio Oy.”
[39] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

could influence this assessment of criticality and lead a Member State to identify a particular media company as a critical entity in the context of NIS2.

The author of this thesis realises that the main research question might not be the most scientific by its nature, but more of a practical one. However, the study aims to provide a deeper understanding of the need for cybersecurity legislation within the EU, and on media companies. This is all to provide context for the main research question, which may first seem as a fairly simple one. However, it has emerged during the planning and conducting of this study that the answer to the main research question is not at all straightforward or simple and that there might not be a single definitive answer to the question. The answer depends greatly on various factors regarding the societal differences of the EU Member States and the differing societal roles of media companies across the EU.

1.5 Structure of the thesis

This thesis is structured into eight chapters.

The first chapter introduces the research topic and explains the scope of the thesis, research methods, and material used, along with the research questions.

The second chapter discusses the European Union's Cybersecurity Strategy and the current operational and legal environment of media companies in the Union. Description and a showcasing of the European Union’s cybersecurity situation and a vision on the future of European cybersecurity brings a contextual briefing to the main research question and helps the reader understand the broader picture around this topic. The second chapter also defines the entity type the thesis is focused on and has a brief introduction to cybersecurity and to different types of cyber threats.

The third chapter focuses on the NIS2 Directive. It explains why a revision of the original NIS Directive was needed and what the revised Directive aims to achieve, defines the scope of application of the Directive, and analyses the feasibility of including media companies to that scope.

The fourth chapter touches on the CER Directive and its impact on the analysis and includes a brief review of some national interpretations and implementation

measures, that have an impact on public broadcasting companies. This chapter also discusses contextual factors that affect the analysis.

The fifth chapter discusses the cybersecurity risk-management measures that the NIS2 Directive requires of entities within its scope, including media companies if they were to fall within the scope of application of the Directive.

The sixth chapter of this thesis discusses critique towards the NIS2 Directive. It provides insight on the predicted effectiveness of the legislation and expresses the author's own analysis of the necessity of the Directive as a legislative instrument for the development of cybersecurity in the European Union.

The seventh chapter provides operational recommendations and best practices for media companies on reacting to the new Directive, both in the cases of whether or not they fall within the scope of application of the Directive. The chapter also discusses how the assessment for the measures should be conducted.

The eighth chapter concludes the thesis and expresses the limitations of the study as well as the author's closing words.

2 Cybersecurity and operational environment of European media companies

The EU is in a phase of renewing its defence and security policies and practices. This is in response to growing geopolitical tensions affecting Europe. As the Commission has stated:

> The global pandemic, Russia's illegal and unprovoked war in Ukraine, hostile economic actions, cyber and infrastructure attacks, foreign interference and disinformation and a global increase in geopolitical tensions have exposed risks and vulnerabilities in our societies, economies and companies that did not exist only a few shorts year ago.[40]

The EU Commission has identified the risks on European economies. This list of four categories of risks is broad and non-exhaustive, but depicts the growing concerns on resilience and security in the EU:

> Risks to the resilience of supply chains, including energy security – Risks of price surges, the unavailability or scarcity of critical products, or inputs in the EU, including but not limited to those linked to the Green Transition, those needed for a stable and diversified energy supply and pharmaceuticals.
>
> Risks to the physical and cyber-security of critical infrastructure – Risk of disruptions or sabotage of critical infrastructures, such as pipelines, undersea cables, power generation, transportation, electronic communication networks, that undermine the secure and reliable provision of goods and services or data security in the EU.
>
> Risks related to technology security and technology leakage – Risk to the EU's technological advancements, technological competitiveness, and access to leading-edge technology, including through malicious practices in the digital sphere such as espionage or illicit knowledge leakage In some cases, technology leakage risks strengthening the military/intelligence capabilities of those that could use them to undermine peace and security, especially for dual-use technologies such as Quantum, Advanced Semiconductors or Artificial Intelligence, and therefore require specific risk mitigation measures.
>
> Risk of weaponization of economic dependencies or economic coercion – Risk of third countries targeting the EU, its Member States and EU businesses through measures affecting trade or investment to bring about a change of policy falling within legitimate policymaking space.[41]

---

[40] European Commission, "European Economic Security Strategy." 1.
[41] Ibid. 4–5.

Cyber- and technology security is recognised as a field that needs active revisioning in order to keep the Union safe and trustworthy, but also to keep the Union's economies competitive and strong. The European Union has several strategical efforts to the challenges it faces. One of them is the EU's Cybersecurity Strategy for the Digital Decade.

2.1 Strategic foundations: The EU's Cybersecurity Strategy for the Digital Decade

In 2020, von der Leyen's Commission and the High Representative of the Union for Foreign Affairs and Security Policy published The EU's Cybersecurity Strategy for the Digital Decade (later Cybersecurity Strategy), which adds to the previous efforts.[42] It is part of a broader framework of the Commissions' strategies and policies.[43] This chapter will discuss the Cybersecurity Strategy as it offers a broad yet clear view of the EU's actions and the evolving landscape that led to the proposal of the NIS2. The Strategy lays the foundation for the revision of the original NIS Directive, and outlines the EU's priorities in cybersecurity, ensuring that critical sectors are well-protected. It provides the rationale for strengthening the legal framework to better address cybersecurity threats across sectors.

The motivation behind the Cybersecurity Strategy is the ongoing digital transformation in the EU, and as the Strategy states; "The EU's economy, democracy and society depend more than ever on secure and reliable digital tools and connectivity."[44] This dependence grows more in the future as governments adopt

[42] In the past, there have also been ways in which the EU has sought to combat unwelcome developments in this field. These have included the first Cybersecurity Strategy of the European Union from 2013, titled An Open, Safe and Secure Cyberspace, the Cyber Act, and the NIS1 among others. These have become obsolete as the times have changed and technology has advanced, and consequently so have the Union's attitude on need and depth of regulation.
[43] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade." 4. The picture consists in particular of; Shaping Europe's Digital Future, the Commission's Recovery Plan for Europe, the EU Security Union Strategy, the Global Strategy for the EU's Foreign and Security Policy, and the European Council Strategic Agenda 2019-2024.
[44] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade." 1.

digital services in their core functions.[45] This change is at risk because cybersecurity measures in the Union area in large are currently not effective enough, as recognised by the Commission.

The types of risks have been discussed above in this thesis, but those specifically discussed and identified in the Cybersecurity Strategy can be summarised to the following: Critical sectors such as transport, energy, health, and finance are increasingly interconnected and vulnerable to cyberattacks, and geopolitical tensions, low cyber readiness, and a lack of cybersecurity skills compound the risks. There is also a lack of collective situational awareness and culture of information sharing in the field of cybersecurity in the EU. The cybersecurity strategy shows how "how the EU will shield its people, businesses and institutions from cyber threats, and how it will advance international cooperation and lead in securing a global and open Internet."[46] Symptoms of the low effectiveness of EU cybersecurity have been shown in recent years in cases such as those discussed above on the governments of Finland and Germany. In 2021, 22 percent of EU enterprises had an ICT-related incident resulting in consequences such as unavailability of ICT services, destruction or corruption of data, or disclosure of confidential data. A significant majority were of non-malicious causes such as hardware or software failures.[47] It is erroneous to assume that all cybersecurity issues have their source in external actors, and that all incidents are damaging.

The Cybersecurity Strategy proposes three instruments which are regulatory, investment and policy. These three instruments will address three action areas which are: "1. resilience, technological sovereignty and leadership; 2. operational capacity to prevent, deter and respond (to cyber threats); 3. cooperation to advance a global and open cyberspace."[48] Let's first have a look at the second and third areas of action.

---

[45] For example, Estonia has adopted electronic governmental services far earlier, and more effective, than most other countries in the Union. This undoubtedly warrants effective cybersecurity which protects the peoples' personal data among other rights, and also democracy and integrity and secrecy of elections. See more on Estonia's e-governance at https://e-estonia.com/solutions/e-governance/e-democracy/. A more comprehensive change is inevitably coming as the EU is establishing the European digital Identity Framework with initiatives like the Digital Identity Wallet, which Member States should issue by the end of the year 2026. See more at https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation.

[46] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade." 1–4.

[47] Eurostat, "ICT Security in Enterprises," Figure 10.

[48] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade." 4.

The second area focuses on building operational capacity to prevent, deter and respond to cyber threats. This includes the establishment of the Join Cyber Unit, which “should enable Member States and EU institutions, bodies and agencies to make full use of existing structures, resources and capabilities and promote a ‘need to-share’ mindset”. The objectives of the Joint Cyber Unit are to become the “heart of EU cybersecurity operational cooperation” and to “act as a backstop where the participants can draw on one another’s support and expertise, especially in the event that various cyber communities are required to work closely together.”[49] The actors involved in the Joint Cyber Unit are “Resilience” units such as ENISA,[50] CyCLONe,[51] Law Enforcement unit EC3,[52] “Diplomacy entities” European External Action Service (EEAS) and Horizontal Working Party on Cyber Issues, and “Defence” units Permanent Structured Cooperation (PESCO) and European Defence Agency (EDA).[53] Time will only tell how these units will in practice share their forces and skills. Along the Join Cyber Unit, EU has other initiatives on this area which are mainly reviewing, supporting, continuing and reinforcing existing programmes on cybersecurity and cyberspace.[54]

The third area of action is cooperation on advancing a global and open cyberspace, which means a space where the rule of law, international law and other norms are followed and respected by states. The EU considers that the state of the multilateral debate on international security in this cyberspace has "deteriorated".[55] To counter this deterioration, the EU seeks to step up its engagement and representation in this debate.[56] EU seeks to be a model citizen in the digital world and aims to provide guidance for those interested. Those not interested, do not have to comply or cooperate, but it is great to see willingness in this field.

---

[49] Ibid, 13–14.
[50] ENISA is the European Union Agency for Cybersecurity.
[51] CyCLONe is the European cyber crisis liaison organisation network.
[52] The European Cybercrime Centre, Established under Europol.
[53] European Commission, Infographic: “Main actors and Networks of cooperation involved in the Joint Cyber Unit. “
[54] European Commission, “The EU's Cybersecurity Strategy for the Digital Decade”. 19.
[55] This could be interpreted to refer to the actions of Russia, China, and the USA in their banning of services from each country.
[56] European Commission, “The EU's Cybersecurity Strategy for the Digital Decade”. 19–23. This action includes inter alia engagement and representation in international standardisation processes and bodies, protecting human and children's rights online, dialogues with global partners, private sector, academia and civil society, and supporting Member States in addressing cybersecurity matters.

In the context of this thesis, the most significant are of action of the Strategy is the first one: Resilience, technological sovereignty and leadership. This area includes the building the European Cyber Shield,[57] ensuring cybersecurity of 5G and future generations of networks, space-based communications in part of the Union's Space Programme,[58] security of IoT,[59] enhancing global Internet Security by supporting the development of a public European DNS resolver service,[60] supporting the education of cybersecurity skilled workforce, and reinforcing the presence of the Union in technology supply chain[61].[62] This area also includes the revision of EU rules on the security of Network and Information Systems, which includes the revision of the NIS Directive. Its aim is to "increase the level of cyber resilience of all relevant sectors, public and private, that perform an important function for the economy and society".[63] The NIS2 Directive, proposed in 2020, represents the revision of the original NIS Directive.

Directives are left to the consideration and implementation of individual Member States, who can then choose the form and methods of implementation. Directives are binding on EU Member States, requiring them to achieve certain results stipulated by directives, which often leads to new obligations for private entities through national implementation. Directives are mainly used to harmonise legislation amongst the EU Member States.[64]

The European Union seeks to step up its relevance in cybersecurity and also undoubtedly in geopolitics, as new and innovative cyber risks emerge and become

---

[57] A collaboration network of Security Operations Centres across the EU which will warn authorities and those that are interested on cybersecurity incidents, "providing a solid mesh of watchtowers, able to detect potential threats before they can cause large-scale damage."
[58] The EU Space Programme was created to support the EU's space policy, to address societal challenges such as climate change and technological innovation, and to support the EU's internal market, innovation and competitiveness by investing in critical infrastructure and breakthrough technologies. Read more at https://defence-industry-space.ec.europa.eu/eu-space/eu-space-programme_en.
[59] Internet of Things, meaning devices connected to the internet.
[60] A European alternative for connecting to the internet. Possibly in response to the Americanisation of internet services in the EU. For example, Statista (https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/) estimated that Amazon (AWS), Microsoft (Azure) and Google Cloud had a combined market share of 67 % amongst cloud infrastructure service providers. Other, but much smaller players are Alibaba, Tencent (both Chinese), Salesforce, IBM Cloud and Oracle (all three from the United States of America).
[61] This is done to reduce dependency of other parts of the world in supply chains.
[62] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade". 6–12.
[63] Ibid p. 5–6.
[64] Ojanen, *EU-Oikeuden Perusteita*, 45–47.

more frequent, originating from countries and organisations hostile towards the Union and its Member States. A revised cybersecurity strategy is an important addition to ensure that progress goes to the direction the Union wants it to go. EU seeks to harmonise the cybersecurity measures and bring all important entities acting in the Union are to a sufficient level of cybersecurity, and to ensure that a certain threshold is met everywhere, in entities that are the most detrimental to the security of the people, economies and the functioning of the internal market. The most apparent downside is that the rapid introduction of regulation and numerous Union entities designated to cooperate on cybersecurity matters could make the cooperation and abiding by the legislation difficult and costly for organisations without cybersecurity expertise.

2.2 Defining the media company in question

The purpose of this chapter is to define the type of entity on which this thesis focuses, and to highlight the variability in the structure and cultural contexts of these organisations across Europe, as well as their links to government bodies. This variation has a significant impact on the final assessment of the research question.

This thesis focuses on the largest media companies active in the Member States. These companies can be seen but are not necessarily specified in national legislation or elsewhere as critical entities. The individual characteristics of a company impact the inclusion to the scope of the Directive. There is considerable variation of organisation and cultural differences in European media companies and in their operating environment.[65] The focus is on the actual media services, not on any other activities the media companies could have. The company provides news and other media content in outlets such television, radio, newspapers or others. The content provided by the company comprises of and focuses mainly on news, entertainment and education. It could also have a public service mandate.

[65] On the differences of European media accountability and the operational environments between countries, see for example *The European Handbook of Media Accountability*, edited by Tobias Eberwein, et al., Taylor & Francis Group, 2017.

The legal form of the organisation is not given restrictions. The company can have ties to a governmental body of the Member State and a somewhat semi-official or even official status as a state-supported, state-owned, or explicitly state-detached public broadcasting company. Some media companies have very clear ties to the State, such as the Finnish Broadcasting Company Yleisradio Oy, the Swedish counterparts SVT, Sveriges Radio and UR, The Italian Rai, and the Lithuanian Lietuvos Radijas ir Televizija. In Sweden, for example, the three public service companies are all owned by a separate foundation called Förvaltningsstiftelsen, the purpose of which is to separate the companies from the State. These three companies are, in principle, independent and not owned by the state or commercial interests. However, the Board of Directors of the Foundation is elected in cooperation by the Parliament and the Government of Sweden.[66] This can be seen as a more of a hybrid-solution on the ownership and perceived relationship to the Government.

The company could have an official or unofficial task of distributing emergency warnings. This task may be based on an assumption or an expectation that the company would be the most or one of the most active media outlets in a possible emergency situation. The task may be also obligatory on the basis of specific legislation. Laki Yleisradio Oy:stä, Act on the Finnish Broadcasting Company, provides that Yle is obligated, along the provision of versatile and comprehensive television and radio programming, as a company responsible for public content service, to broadcast official announcements, and to prepare for the operation of television and radio services in exceptional circumstances.[67]

2.3 The current legal environment for media companies

To better understand the context of where NIS2 will step onto, it is beneficial to set the scene and understand the legislative framework in which media companies

[66] UR, “Om public service.”
[67] 7.7 § of Laki Yleisradio Oy:stä 1380/1993 Same nature of legislation is also laid elsewhere in Finnish law. Valmiuslaki 1552/2011 states that publishers and broadcasters are liable to, without compensation, publish official announcements made by the authorities, on matters which must be brought quickly to the attention of the entire population or residents of a particular area. Laki vaaratiedotteesta 466/2012 stipulates that emergency warnings are sent to Yleisradio Oy for further distribution through radio and television broadcasts. Similar regulation on public service media has also been laid down in Laki sähköisen viestinnän palveluista 917/2014.

operate in. In this chapter I will look at the legislation currently affecting media companies, in the area of cybersecurity and also in general, but not with the goal of exhaustively listing all media regulation.

Media is sometimes referred to as the Fourth Estate, meaning that media is understood to have significant political influence,[68] along the three Powers of State. This refers to the doctrine of the separation of powers, with which Baron de Montesquieu is most often associated, although he did not invent the idea,[69] but rather developed the theories of John Locke and Thomas Hobbes to include the judicial power among the legislators and their enforcers.[70]

The most prominent principles of trusted media activities are transparency and accountability and the freedom of press. The ownership arrangements of media entities must be transparent, in order for people to decide if the source is trustworthy and accountable. Examples of EU instruments on these matters are the Audiovisual Media Services Directive (EU) 2018/1808[71] which regulates the content produced, and the European Media Freedom Act (2024/1083) which stipulates the freedom of media.[72] EU State aid rules are applicable to public service broadcasting[73],[74] as is the Directive on the transparency of financial relations between Member States and public undertakings as well as on financial transparency within certain undertakings

[68] Cambridge Dictionary: "the Fourth Estate."
[69] Vile. *Constitutionalism and the Separation of Powers,* 83.
[70] Siemers, The Myth of Coequal Branches: Restoring the Constitution's Separation of Functions. 37.
[71] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.
[72] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).
[73] European Commission, "Communication from the Commission on the application of State aid rules to public service broadcasting."
[74] Parcu and Brogi, "Introduction to Research Handbook on EU Media Law and Policy: understanding the EU approach to media law and policy. The scope of the Handbook and a presentation of the contributions," 5.

(2006/111/EC).[75] The EU Artificial Intelligence Act[76] regulates media companies that use AI systems.[77]

General Data Protection Regulation (EU) 2016/679, hereafter GDPR,[78] governs accountability and transparency,[79] but focuses on data protection matters, along with the ePrivacy Directive (which is currently under revision to become the ePrivacy Regulation).[80] The GDPR also requires all companies, including those in the media sector, to implement measures to protect personal data against unauthorized access, breaches, and other related threats.[81]

Regulation on the European media market is fragmented, and poses difficulties for media companies, in particular if they are willing or already operate in another Member State.[82] There is a risk that entities will be "suffocated" by excessive and overly intensive regulation. The European Union has been accused of over-regulation on several occasions,[83] and the European Council has acknowledged this and pointed it out to the Commission.[84]

In the annual report of Yleisradio, the company states that "Yle has strong technical and functional capabilities to respond to security threats, and these capabilities are continuously being improved as part of the national preparedness network. In 2023, the company made significant progress in strengthening cyber and information security. Yle was able to successfully defend itself against information security attacks brought about by the changing world situation. Cyber security was improved in the

---

[75] Commission Directive 2006/111/EC of 16 November 2006 on the transparency of financial relations between Member States and public undertakings as well as on financial transparency within certain undertakings.
[76] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
[77] Preamble (4) Artificial Intelligence Act.
[78] Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation).
[79] Alén-Savikko, "Transparency in algorithmic journalism: from ethics to law and back," 44–45.
[80] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[81] See i.e. Articles 32–34 , and 25 5(1)(f) GDPR.
[82] Preamble (5) European Media Freedom Act.
[83] Accusations on over-regulation for example at: https://swissgrc.com/en/the-eus-ai-dilemma-innovation-or-over-regulation/and https://www.uschamber.com/international/how-europe-pays-a-high-price-for-its-overregulation-of-the-digital-economy.
[84] European Council, "Special meeting of the European Council, 17 and 18 April 2024."

company in many ways, including the use of AI to proactively fight threats."[85] Organisations will have to disclose data breaches in their annual sustainability reports for the financial year 2024, in reports published in 2025. This is due to the CSRD Directive[86],[87] along with the GDPR and NIS2, which supplement the cybersecurity reporting duties. NIS2 has the effect of potentially standardising a level of higher quality for cybersecurity reporting, as it mandates that management bodies to have sufficient knowledge of cybersecurity measures and to approve the measures that are to be taken.[88] This could translate into better and clearer reporting on these matters.

2.4 Types of cybersecurity threats

To better understand the cybersecurity threats and risks this thesis focuses on, and the measures the EU is imposing on critical entities, a basic understanding of the terminology and of incident prevention tactics has to be established.

The term cybersecurity is broad and is used to describe the countermeasures taken to deter or defend against cyberthreats and cyberattacks. The term cybersecurity, and even more the word "cyber",[89] can be quite ambiguous. This thesis focuses on matters included in the EU definition of the term. In the NIS2 cybersecurity is defined in the Article 6 (3), which refers to the definition of Article 2, point (1), of the Regulation (EU) 2019/881, hereafter EU Cybersecurity Act;

> activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.[90]

Cyber threat is defined in Article 6(10) of the NIS2 Directive as is defined in Article 2, point (8), of the Cybersecurity Act;

---

[85] Yleisradio Oy, Annual report 2023, 82. Note the reported usage of AI to fight cyber threats.
[86] Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting.
[87] Boggini, "Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework", 2.
[88] Ibid, 7.
[89] For example, used on the Tesla Cybertruck, an electric pickup truck by the American manufacturer.
[90] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

> meaning any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.

By network and information systems (NIS), the EU means, as defined in Article 4(4) of NIS1;

> (a)an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC (repealed by Directive (EU) 2018/1972, Article 2(1)); *transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;*
>
> (b)any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or
>
> (c)digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

There are many different kinds of cyberattacks done by many different types of attackers. The types of attackers can be divided into different categories based on the party they represent. Some are more organised, others work by themselves, and there are external attackers, but also internal attackers, meaning those who are already inside the organisations before the attack. There are terrorist and organised criminal groups which can have varying motifs behind their actions. New players are called script kiddies and lone wolves. There are also hacktivists with often political objectives, and security agencies working on behalf of states.[91] White-hat hackers are professionals with good intentions behind their actions, that work with the permission of the owner of the system to find vulnerabilities. Black-hats have their own purposes and no permission on exploiting those same vulnerabilities.[92]

---

[91] Sutton, *Cyber Security: The Complete Guide to Cyber Threats and Protection*, 133–139.
[92] Eric Filiol, "Francesco Mercaldo, Antonella Santone. A Method for Automatic Penetration Testing and Mitigation: A Red Hat Approach", 2041.

Ransomware is a type of cyberattack that is used to demand something from the victim, usually money or other assets, in order to let the user out of a situation a malicious software has set on their device. The attacker might threaten to delete data or cause other damage to an individual or their organisation if the ransom is not paid.[93] Other typical attacks types are Denial-Of-Service attacks or DoS attacks,[94] Botnets which connect a large number of victims' computers which can be then accessed remotely for different purposes like DoS attacks, Brute force attacks that persistently use force to solve something, like a user password, Wireless network attacks that attack the infrastructure of network technologies, and the usage of backdoors that are normally used to make changes to the code of a program while testing, but also to access the code if the door is not removed.[95] This list is not exhaustive.

These various and ever-renewing types of attacks are addressed by implementing effective incident[96] prevention measures. In cybersecurity, incident prevention is the goal, but detection and response are the reality. This is where incident handling and response come to action. One widely used incident response model, but not the only one in use,[97] named Classic or the PICERL model, has six steps: 1. Preparation, which refers to the measures done before the incident has occurred; 2. Incident Detection or Identification, usually done by the user for example by calling the help desk; 3. Containment of the compromised systems, by for example taking compromised websites offline; 4. Eradication of the damages, meaning for example stopping the attackers' processes or changing user passwords; 5. Recovery from the incident by getting the systems back running; and 6. Lessons learned, meaning fixing the vulnerabilities, and preparing a final report.[98] Models like this are standard approaches to cybersecurity measures done by organisations.

---

[93] Berkeley, "Frequently Asked Questions – Ransomware."
[94] A further developed version of this attack type also exists, DDoS or Distributed Denial of Service attack.
[95] Sutton, *Cyber Security: The Complete Guide to Cyber Threats and Protection,* 150-160.
[96] The term incident is used as an umbrella term for cybersecurity events in cybersecurity. Article 6(6) NIS2 defines incident as "an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems."
[97] There are no one-size-fits-all approaches to incident response processes. More nuanced and dynamic approaches do exist.
[98] Murr, SEC504.I Incident Response and Computer Crime Investigations, 22.

An adequate level of cybersecurity is important for all companies that are connected to any network, which makes it important for virtually every company today. The greater the size and significance of a company, the more substantial the potential for damages and societal impact. This is why also media companies have to ensure a competent level of cybersecurity. Adequate measures ensure that the entity is able to recover from attacks. Naturally, there are also other risks that companies have to mitigate and develop risk-management measures for. Yleisradio stated in its 2023 annual report that its identified risks were a decline in society's support for the company in its current form, impact of artificial intelligence on Yle and its operating environment, cyber threats and information security risks as well as threats towards journalists. In 2023, Yle was subjected to a distributed denial-of-service (DDoS) attack. However, the company asserts that the attack was successfully mitigated. Yle stated that incident preparedness and incident recovery will be developed, and that information security monitoring and response capabilities were improved. A large-scale migration of services into cloud was also done.[99] These post-incident actions listed reflect the last two steps of the incident response model described above.

This shows that cyberthreats and attacks are a prevalent risk for media companies, and that there needs to be an adequate system to detect and investigate incidents. For media companies, cybersecurity is also connected to the reliability of the data used for news production, which can be affected or distributed by attackers or groups conducting hybrid threats and hybrid influencing such as cyberattacks, spreading disinformation, hate speech and deepfakes.[100]

Europe is actively renewing its cybersecurity preparedness. The NIS2 Directive is an integral part of this project, and the Cybersecurity Strategy speaks the intention of the EU on its measures to enhance the security of Europeans, and to safeguard its position in geopolitics. Media companies are already regulated in their everyday functions, but cybersecurity is not specifically regulated as explicitly as the NIS2 Directive seeks to regulate critical entities. The possibility of inclusion of media companies to the scope of the Directive sits well in the legal operating environment of the media sector. Requiring the most critical media companies to implement effective

[99] Yleisradio Oy, Annual report 2023, 90-91.
[100] Hybrid CoE, *Countering Disinformation: News Media and Legal Resilience*, 12–13.

cybersecurity measures helps in protecting the dissemination of important information in Europe.

3 Evolution and scope of application of the NIS2 Directive

This chapter discusses the NIS2 Directive. The chapter first explains what was lacking in the original NIS Directive and what are the main additions in NIS2. Secondly, it examines the scope of the Directive and the possibility of including media companies in definitions of any sector of critical entities listed in the Annex I and II of the Directive. The aim is to strictly utilise the grammatical approach in this chapter, meaning the exact wording of the legal text, and to provide the foundation on answering the main research question: *Do media companies fall under the scope of the NIS2 Directive?* The analysis of this chapter will therefore not go further into the other interpretation methods discussed earlier. As admitted before, pure non-contextual interpretation of any legal text does not exist, and this is why the contextual influences on the interpretation of the scope of the Directive, i.e. teleological and systemic interpretations, are discussed in Chapter 4 of this thesis.

3.1 Revision of the NIS1 Directive

The original NIS Directive was aimed to achieve a high common level of security of network and information systems across the Union, largely same as the revised NIS2 Directive.[101] Several shortcomings became apparent over time, and the European Commission has admitted that the original NIS Directive did not meet this goal. Instead, the situation was characterised as follows:

> insufficient level of cyber resilience of businesses operating in the EU, inconsistent resilience across Member States and sectors, insufficient common understanding of the main threats and challenges among Member States and lack of joint crisis response.[102]

Four key changes can be identified in the new NIS2 Directive compared to the original NIS Directive. These changes are enlargement of the scope, new and revised risk management measures and updated reporting obligations, new supervisory

[101] Article 1(1) of the NIS1 Directive. A notable revision is the usage of the term cybersecurity in the Article 1 of the NIS2 Directive instead of "security of network and information systems" used in Article 1(1) of the NIS1 Directive.
[102] European Commission. "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – FAQs."

regime and harmonised penalties towards non-compliant entities.[103] The enlargement of the scope means covering more entities in existing sectors of the Directive and including multiple new sectors to the legislation.[104] It is precisely this revision of the scope that has prompted organisations to consider their position on the Directive and the possibility of new obligations under subsequent national legislation. The same applies to media companies. The extension of the scope raises the question of whether they would be covered by the Directive. This is a good thing, as not being on top of new legislation can bring unpleasant surprises.[105] NIS1 did not include media companies in its scope, as the sectors it concerned did not have any correspondence to functions of media companies, unlike the revised NIS2 Directive potentially has.

This widening could be interpreted as a step towards EU legislation governing the cybersecurity of all Union entities in the future.[106] In the opinion of the author, this widening is a positive development. Achieving a certain baseline in cybersecurity matters should be the absolute minimum for all organisations, and legislation could be a key point in assisting organisations in reaching that baseline. The introduction of more mandatory measures is also a positive development, along with the updated supervision.

NIS1 was considered to give too much leeway for EU Member States in determining the cybersecurity measures and incident reporting requirements, and not considered to ensure effective monitoring and enforcement.[107] This is in comparison to the cyber security situation in Europe today, which has changed since the legislation was introduced. It seems then that NIS1 did not introduce significant new requirements for companies that already had cybersecurity measures in place, while at the same time failed to adequately obligate those that did not. The scope of NIS1 was

---

[103] Schmitz-Berndt, Chiara. “One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive.” 291.
[104] Sievers, “Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations,” 224.
[105] NIS2 and subsequent national legislation was recently discussed in Helsingin Sanomat by Henri Viljasjärvi, Director of Business Development at Digita Oy. See https://www.hs.fi/mielipide/art-2000010777469.html. Only in Finnish.
[106] Vandezande, “Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor,” 6.
[107] European Commission, “Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, Explanatory memorandum,” and preambles (4), (6) and (7).

insufficient to address the evolving situation in Europe, which has been affected by the global health crisis of Covid-19 and a series of geopolitical disruptions.

Implementation of the NIS1 was fragmented, and Member States had a large variety in the identified number of essential operators. In the evaluation of the Commission on NIS1 it was observed that the differences in identifying the entities led to "different levels of maturity in dealing with cybersecurity risks".[108] Finland, for example, identified a very large number of operators of essential services in the health sector of the NIS1. The number of operators of essential services in Finland was 10897, while the total amount in all other Member States combined was 4925.[109] Finland's essential operator identification methodology led to an unusually high number of operators of essential services, highlighting the wide variation in how NIS1 was implemented. This is further illustrated by the actions of Germany and Italy, which adopted stricter cybersecurity obligations than the NIS1 warranted. This led to a situation where these Member States have already introduced cybersecurity management and reporting obligations that are already very much in line with the NIS2 or require very little modification.[110] These divergences in implementation resulted to significantly differing operational environments between the Member States, which does not contribute to the functioning of the internal market. A mechanism on levelling the playing field was therefore needed. This mechanism was introduced by stipulating that the size of an essential or important entity determines its inclusion in the scope of the revised Directive,[111] although there are exceptions to this rule, which will be discussed later in this thesis.

As the means of implementation of the Directive are left to the Member States, Article 5 on minimum harmonisation of the Directive states that (the Directive) "shall not preclude Member States from adopting or maintaining provisions ensuring a higher

---

[108] European Commission, "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148", 5.
[109] European Commission, "Report from the Commission to the European Parliament and the Council: assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems." Annex 4.2. Numbers of services and OES identified by each Member State.
[110] Schmitz-Berndt and Chiara. "One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive," 307–308. Modifications are needed to the national legislations, in particular to the incident notification timelines required.
[111] Sievers, "Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations," 226.

level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law." What follows is that the Member States are given the freedom to adopt measures of higher levels of cybersecurity. Finland seems to have been taken the stance of not implementing anything more than the minimum requirements of the Directive, and by using the national margin to the full extent.[112] This is entirely acceptable as the Directive is a minimum harmonisation directive but could work against the goal of achieving a common level of cybersecurity, as some Member States could end up having a higher standard of security, and some choose to stick to the minimum level. What is important in this, is that the minimum level is adequate enough.

On top of the broadened scope, NIS2 categorises entities based on their level of importance into two groups; essential entities and important entities, instead of the categorisation of NIS1 which consisted of operators of essential services and digital service providers. The Directive also updates reporting and supervisory provisions, addresses cybersecurity in supply lines, and enhances co-operation between EU Member States in cybersecurity matters.[113] The actual measures are discussed later in this thesis.

The broadening of scope in NIS2 suggests a trend towards a more comprehensive cybersecurity framework across the Union. It has been estimated that there will be around 160 000 entities under the scope of the revised Directive. This marks a significant shift in the way cybersecurity risks are managed and reported in Europe. A much wider range of sectors will be held to strict cybersecurity standards through legislative action. This may also influence the general attitude and atmosphere surrounding cybersecurity issues among Europeans. A further discussion of this development can be found in Chapter 7 of this thesis.

---

[112] HE 57/2024 vp, 1.
[113] European Commission. "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – FAQs."

3.2 Scope of application of the NIS2 Directive

This chapter aims to clarify the scope of application of the NIS2 Directive, particularly focusing on critical sectors outlined in Annex I and Annex II of the Directive. By examining these sectors and the specific criteria for inclusion, we gain a comprehensive understanding of the Directive's scope. First, I will have a look at the conditions of the general scope, and after that assess the specific applicability of the sectors on media companies, the possible specifics of which were defined in chapter 2.2.

Article 2(1) of the NIS2 states that the Directive

> applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.

The above referred Article 2 of the Annex to Recommendation 2003/361/EC states that

> 1. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.
>
> 2. Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.

This means that medium sized enterprises have fewer than 250 persons employed and have an annual turnover and/or balance sheet total between EUR 10 million and EUR 10 million. The enterprise exceeds the SME category if it has an annual turnover of over EUR 50 million and/or an annual balance sheet total that exceeds EUR 43 million. Both the number of employees and the turnover and/or balance sheet thresholds have to be met.

Article 2(2) defines that the size of the company does not have any effect when determining the applicability of the Directive, if referred to in the annexes I and II, and if any of the following conditions is met.

> (a) services are provided by:

(i) providers of public electronic communications networks or of publicly available electronic communications services;

(ii) trust service providers;

(iii) top-level domain name registries and domain name system service providers;

(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;

(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;

(f) the entity is a public administration entity:

(i) of central government as defined by a Member State in accordance with national law; or

(ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.

Article 2(3) of the NIS2 Directive states that "Regardless of their size, the Directive applies to entities identified as critical entities under Directive (EU) 2022/2557" or the CER Directive. This warrants that this thesis will also have to look at the scope of application of the CER Directive. This is done later in chapter 4.1.

Let's now have a look at the Annexes of NIS2, which have the sectors of entities in the scope of the Directive. The annexes are shown here as a list of the sectors, with a brief description of the entities they concern.

3.2.1 Annex I: Sectors of high criticality

Energy: This sector consists of subsectors electricity, district heating and cooling, oil, gas, and hydrogen, all crucial for the continuous supply of energy.

Transport: This includes subsectors of air, rail, water, and road transport, essential for the movement of goods and people.

Banking and financial market infrastructures: This sector includes credit institutions and operators of trading venues and central counterparties, key for financial stability.

Health: This sector includes healthcare providers, laboratories, research and development, pharmaceutical manufacturers, and manufacturers of medicinal devices, this sector is vital for public health.

Drinking water: This consists of suppliers and distributors of water intended for human consumption, essential for public health.

Waste water: Including undertakings that collect, dispose of, or treat urban, domestic, or industrial wastewater. This sector is crucial for environmental and public health.

Digital infrastructure: This sector includes Internet Exchange Point providers, DNS service providers (excluding operators of root name servers), TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, trust service providers, providers of public electronic communications networks, and providers of publicly available electronic communications services, all essential for digital connectivity.

ICT service management (business-to-business): Consisting of managed service providers and managed security service providers, this sector supports other businesses with critical IT services.

Public administration: This includes public administration entities of central governments and regional public administration entities as defined by Member States, essential for governance and public services.

Space: This sector consists of operators of ground-based infrastructure, owned, managed, and operated by Member States or private parties, that support the provision of space-based services, excluding providers of public electronic communications networks, essential for satellite communication and navigation.

3.2.2 Annex II: Other critical sectors

Postal and courier services: This includes postal service providers and courier services, essential for communication and commerce.

Waste management: Consisting of undertakings carrying out waste management, this sector is crucial for environmental protection.

Manufacture, production and distribution of chemicals: This sector includes undertakings involved in the manufacture and production of chemical substances or mixtures, essential for various industries.

Production, processing and distribution of food: This sector consists of food businesses engaged in wholesale distribution and industrial production and processing of food, vital for food security.

Manufacturing: This sector includes manufacturers of medical devices, in vitro diagnostic medical devices, computer, electronic and optical products, electrical equipment, machinery, motor vehicles, trailers, semi-trailers, and other transport equipment, essential for various industries.

Digital providers: This includes providers of online marketplaces, online search engines, and social networking services platforms, integral to modern digital services.

Research: This sector consists of research organizations, important for scientific and technological advancement.

3.3 Applicability of the NIS2 Directive to media companies

We can now conclude that NIS2 is applicable to an entity if: 1) Referred to in Annex I or II NIS2; 2) it qualifies as a medium sized enterprise, exceeds the ceiling for medium-sized enterprise, or fulfils any of the conditions of Article 2(2) NIS2 or (3) The entity is identified as a critical entity in the CER Directive. The entity also has to carry out their activities within the European Union.

Let's now compare the scope of application to media companies as defined before. Individual assessment must always be made, and no individual conclusions can be made from this assessment. This assessment does not cover all media companies.

3.3.1 Size of the entity

First let's go through the size criteria of the Directive, which is the first criteria to look at when determining the scope, as it acts as a principal divider between the entities not in scope and those included in the scope of NIS2. In the case of Yleisradio Oy, we can see that the company had an annual turnover of over EUR 500 million.[114] As another example we can look at the Swedish Broadcasting Company SVT's numbers and see that this company also exceeded the EUR 50 million turnover threshold, with its EUR 490 million turnover.[115] We will assume that other companies in question in the EU are similar to these two in this aspect, and will exceed the threshold of at least the EUR 10 million turnover or balance sheet total.

---

[114] Yleisradio Oy, Annual report 2023. 4.
[115] SVT, "SVT och pengarna - Året med SVT", The turnover was approximately SEK 5,5 billion. Rounded and converted to Euros by the conversion rate as of 21 February 2024, it is approximately 490 million Euro.

Next let's have a look at the second clause in the paragraph, the threshold for number of employees. Yleisradio Oy had 2915 employees at the end of year 2022[116] and SVT had about 2100 employees in the year 2024 at the time of writing this thesis.[117] These companies exceed the threshold of 50 employees. We will assume that most media companies which could be considered as critical entities also meet these thresholds.

If the media company meets any of the criteria of Article 2(2) or 2(3) of the Directive, and is included in the Annex I or II, the size of the company does not have an effect when determining the applicability of the Directive. The assessment is not made in this thesis, as it is out of the focus. If the thresholds discussed above are not met, the entity has to make this assessment. If an entity does not meet any of these criteria, it is not in the scope of the NIS2.

3.3.2 Applicability of the sectors of Annex I and II to media companies

This chapter explores which sectors from Annexes I and II of the Directive might apply to a media company that plays a crucial role in providing trusted news, using definitions from Article 6 of the Directive for a detailed assessment. To determine the most relevant sector for a media company, four potential sectors have been chosen: Digital Infrastructure, Digital Providers, Public Administration, and Research. These sectors are selected based on their relevance to the operational and societal role of media companies. There could be other potential sectors for media companies if definitions are stretched wider, but it is best to leave further speculation out of this thesis.[118] A detailed analysis of the definition is needed in order to identify if there are any possible subsectors media companies could be included in, and on what conditions.[119]

---

[116] YLE, "Henkilöstön avainluvut 2022."
[117] SVT, "Jobba här."
[118] This selection is already quite wide, and any further expansion would be out of the scope of the thesis.
[119] To address a possible misunderstanding of media companies' inclusion to the subsector of "data centre service providers" of the digital infrastructure sector; media companies could own and operate data centres for their own usage, for content creating or other purposes. The NIS2 Directive excludes these kinds of data centres from the definition as stated in preamble (35); "term 'data centre service' should not apply to in-house corporate data centres owned and operated by the entity concerned, for its own purposes. "

3.3.2.1 Digital infrastructure

Let's start by having a look at the sector Digital infrastructure and its subsectors. Media companies' dependence on digital infrastructure is significant. The security and resilience of these infrastructures is crucial for the continuity of the services media companies provide. This would indicate that this sector would likely be applicable to media companies. Media companies typically do have infrastructure in its traditional form, meaning buildings and vehicles, but here the focus is on digital infrastructure.

The sector is divided into subsectors as defined in the previous chapter. From the subsectors listed we can rule out everything else but content delivery network providers, providers of public electronic communications networks and providers of publicly available electronic communications services. Other subsectors are related to internet services infrastructure or trust services which media companies are typically not involved in. These entity types are defined in Article 6 NIS2, which also has definitions for the other sector's entity types.

Article 6(1(32)):

> 'content delivery network' means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers.

The last few words of this definition are crucial here. The definition is that the network provider provides the network on behalf of content and service providers. By interpreting the wording of the definition strictly and accurately, media companies would be left outside of the scope. It could be argued that a media company could well have a network of servers that is geographically distributed, and therefore has to protect their network, which would be correct. However, media companies are left outside of the scope, because a content delivery network entity would have to provide the services on behalf of content and service providers. Media companies in the context of this thesis are in the definition of the latter.

Article 6(1(36)) states that

> 'public electronic communications network' means a public electronic communications network as defined in Article 2, point (8), of Directive (EU) 2018/1972.

The referred Article 2(8) of Directive (EU) 2018/1972 defines this network as

> an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services which support the transfer of information between network termination points.

Here we have to differentiate between usage and ownership of the network infrastructure. If the media company does not own the network, the primary responsibility for ensuring the cybersecurity of that network would lie with the owner or operator of the network (e.g. the telecom provider). A media company would likely be a customer of that network service provider, and thus not own the network used.

A media company would be left outside of the scope if it does not own the public electronic communications network supporting the transfer of information between network termination points. If this media company would own the network used, meaning that the media company would own and run a broadcasting network, the Directive could apply to the company based on this condition. However, this is usually not the case as it is more common that companies purchase network services from specialised providers. These providers then have to make sure that their cybersecurity measures comply with regulatory requirements, and this is most probably also required on service contracts made between the service provider and media company. The subsector of providers of public electronic communications networks has potential to include some media companies in the definition of digital infrastructure.

Article 6(1(37)) states that

> ‘electronic communications service’ means an electronic communications service as defined in Article 2, point (4), of Directive (EU) 2018/1972.

The referred Article defines this service as

> a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:
>
> (a) ‘internet access service’ as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
> (b) interpersonal communications service; and
> (c) services consisting wholly or mainly in the conveyance of signals

> such as transmission services used for the provision of machine-to-machine services and for broadcasting.

Notable here is the exclusion of "services providing, or exercising editorial control over content transmitted…". This means that entities that have editorial control over, or provide the content transmitted are ruled out of the scope of this definition. Therefore, media companies do not fit in the definition of electronic communications services.

Media companies rely heavily on digital infrastructure. However, the specific definitions of subsectors of that sector in NIS2 largely exclude them from that sector. An exception is if a media company owns a public electronic communications network. This network should fulfil the definition of the EU legislator. This is usually not the case, as media companies typically outsource network services to specialised network providers, but this is a notable possibility and could mean that some media companies are in the scope of application of NIS2 under this provision.

3.3.2.2 Digital providers

Let's now have a look at the sector of digital providers. Many media companies use or operate digital platforms to distribute their content. This sector is particularly relevant for media entities that have a strong online presence and rely on digital channels to reach their audience, making them in principle, and in natural language, service providers in the digital world.

The sector is divided to subsectors of providers of online marketplaces, providers of online search engines, and providers of social networking services platforms. We can immediately rule out online search engines, as these are services such as Google or Bing. The same applies to online marketplaces, as media companies do not usually have such a platform. As for the last possibility, social networking service platforms, Article 6(33) of the NIS2 Directive states that

> 'Social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations.

Media companies do typically not have a service as wide as defined here, but often have a possibility for users to comment or share content. Typically, media companies

of the scope of this thesis have able users to comment on news articles or videos uploaded online. This function is not significant enough to be interpreted as constituting a social networking services platform. The additional interaction that the media content could be the subject of discussion, takes place on other platforms, such as Facebook or Reddit. Inclusion of media companies to the digital providers sector can be ruled out, and therefore media companies are out of the scope of the sector digital providers.

3.3.2.3 Research

Let's now look at the research sector, which could, if understood broadly, include media companies, as they might engage in research activities related to media consumption trends, audience behaviour, or content development. Media organisations and companies with investigative journalism functions might also be included here due to their contribution to research. The definition of research organisations is in Article 6(41) NIS2, and states that

> 'research organisation' means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.

The wording of this definition completely excludes media companies from this sector, as their primary objective is not applied research or experimental development for commercial purposes. Therefore, media companies are not included in the research sector listed in Annex II of NIS2. Media companies are not included in the research sector, but they may still be subject to other legislation concerning their research activities, such as data protection legislation and legislation on consumer behaviour analysis.

3.3.2.4 Public administration

At a first glance, media companies should not be in the definition of governmental entities. However, public broadcasting companies can be affiliated with government entities, as discussed before. This could make them, in principle, eligible to be counted in the sector of public administration, or at least be seen, in natural language and possibly in public perception, as part of public administration. Their classification as public administration entities and inclusion to this sector depends on

the definition of public administration of the NIS2, provided they are an entity of central or regional government in accordance with the national law, as defined in the Annex I.

Let's now have a look at this sector and its definitions. Article 6(35) NIS2 defines a public administration entity as

> an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:
>
> (a)it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;
>
> (b)it has legal personality or is entitled by law to act on behalf of another entity with legal personality;
>
> (c)it is financed, for the most part, by the State, regional authorities or by other bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities or by other bodies governed by public law;
>
> (d)it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

Criterion (a) and (b) are relatively self-explanatory. Criterion (c) has a sort of an extension to the scope as it includes those that are financed, for the most part, by the State. What the most part means, is not clarified. The Cambridge Dictionary defines the word "most" as the "biggest number or amount of; more than anything or anyone else."[120] This suggests that the amount is more than half of the total financing. Therefore, the media company should be at least 50 % financed by state.

Even if the criteria (a), (b) and (c) would be met, fulfilling the criteria (d) seems unlikely for media companies. Criterion (d) requires entities to be able to exercise public powers, meaning the ability to make administrative or regulatory decisions that impact the rights of natural or legal persons in the internal market of the European Union This criteria rules a significant number of media companies out of

[120] Cambridge dictionary, "most."

the definition.[121] Media companies typically do not have the authority to make administrative decisions affecting the rights of natural or legal persons.

One area where media companies, in particular those with a public service mandate, can be considered to have public power is in public procurement procedures. Public procurement is the process that governmental and state-owned public companies have to go through in order to purchase goods, services, or work.[122] Public procurement is regulated by law, and the EU has its own set of public procurement legislation to set out minimum harmonised public procurement rules for businesses across Europe.[123] The goal of regulated public procurement is to increase competition in the internal market of the European Union by opening national public procurement markets to the markets of other Member States[124],[125] and in doing so, increase the efficiency of public funds usage in the Member States.[126] Public procurement legislation in the EU Member States is based on Directive 2014/24/EU on public procurement,[127] Directive 2014/25/EU on procurement by entities operating in the water, energy, transport and postal services sectors,[128] and Directive 2014/23/EU on the award of concession contracts[129].[130]

There is an exclusion for media companies regarding the public procurement processes. In Article 10(1)(b) Directive 2014/24/EU, it is provided that service contracts

> in acquisition, development, production or co-production of programme material intended for audiovisual media services or radio media services, that

---

[121] Note that the group of entities discussed varies and is by no means unified. This further emphasises the necessity of a case-by-case assessment for each individual media entity.
[122] OECD, "Public Procurement – OECD."
[123] European Commission, "Public Procurement."
[124] Caranta, Edelstam, and Trybus, EU Public Contract Law: Public Procurement and Beyond, 65.
[125] Public procurement has been also identified as a serious challenge to the functioning of a competitive single market with the possibility of rendering the functioning less effective and restricted for entities willing to offer services. For more information, see Lianos and Odudu. Regulating Trade in Services in the EU and the WTO: Trust, Distrust and Economic Integration. 147–148. It seems that public procurement can be beneficial if implemented correctly but could have negative effects on competition.
[126] Eskola, Kiviniemi, Krakau, and Ruohoniemi. Julkiset Hankinnat, 19.
[127] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.
[128] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC.
[129] Directive 2014/23/EU of the European Parliament and of the Council of 26 February 2014 on the award of concession contracts.
[130] Eskola, Kiviniemi, Krakau, and Ruohoniemi. Julkiset Hankinnat, 20.

are awarded by audiovisual or radio media service providers, or contracts for broadcasting time or programme provision that are awarded to audiovisual or radio media service providers[131]

are excluded from the Directive 2014/24/EU. The actions explained in Article 10(1)(b) Directive 2014/24/EU are only a part of the service public broadcasting companies provide, so this exclusion does not rule out the possibility of inclusion of media companies to the sector of public administration. Conversely, this exclusion demonstrates that media companies are subject to some public procurement legislation.

Public procurement decisions are accompanied with a notice of appeal, as is often the case with administrative decisions. This is to ensure access to justice and the possibility of appeal if the person receiving the decision considers it appropriate to do so. This means that public broadcasting companies that have to abide by public procurement in procurement other than that defined in Article 10(1)(b) Directive 2014/24/EU, can be seen as having some public powers. For example, in Finland, public procurement law states that the contracting entity must attach a notice of appeal to its decision,[132] and the administrative procedure act states that any decision, if applicable, must be accompanied with a statement of grounds for appeal.[133]

There is Union case law regarding public procurement and infringements of rights of contractors. In Beentjes v. Netherlands the European Court of Justice (CJEU) examined whether a Dutch public procurement decision violated EU (then EEC) law. The procurement contract had a criterion that required the winning contractor to employ long-term unemployed persons. The CJEU ruled that the additional condition was incompatible with the EU procurement Directive if it leads to discrimination on

---

[131] Preamble (23) Directive 2014/24/EU elaborates on the exclusions:
"The awarding of public contracts for certain audiovisual and radio media services by media providers should allow aspects of cultural or social significance to be taken into account, which renders the application of procurement rules inappropriate. For those reasons, an exception should therefore be made for public service contracts, awarded by the media service providers themselves, for the purchase, development, production or co-production of off-the-shelf programmes and other preparatory services, such as those relating to scripts or artistic performances necessary for the production of the programme. It should also be clarified that that exclusion should apply equally to broadcast media services and on-demand services (non-linear services). However, that exclusion should not apply to the supply of technical equipment necessary for the production, co-production and broadcasting of such programmes."
[132] Laki julkisista hankinnoista 126 §.
[133] Hallintolaki 47 §.

grounds of nationality.[134] Another case dealt with prohibiting a contractor on submitting a tender on work that they have completed preparatory works for. The Court held that this was disproportionate for achieving the objective of equal treatment of tenderers.[135] There has also been case with complete absence of competitive tendering, which would infringe the rights of other competent bidders.[136] These cases show the clear potential for public procurement affecting the natural or legal persons' rights in the cross-border movement of persons, goods, services or capital.

Public procurement legislation applies to only a small part of the actions of media companies and excludes the production of content. This argues both pro and contra the inclusion of media companies to the sector public administration and to the scope of application altogether. The interpretation result depends on the value given to that small amount of public power. Based on the wording alone, the author's analysis is that public service broadcasters fall within the scope of the Directive, as neither criterion (d) nor the preamble to the Directive explain how much public power an undertaking must have to be considered meeting the criterion. Rather, the analysis is based on a question of yes or no.

It is also important to note that Article 2(5)(a) of the NIS2 Directive states that "Member States may provide for this Directive to apply to: public administration entities at local level…," This indicates that if a Member State were to classify a media company as a local level public administrative entity, that company would be within the scope of the Directive, regardless of whether it meets the criteria discussed here.

To conclude, public procurement processes can affect natural or legal persons' rights in the cross-border movement of persons, goods, services or capital, and media companies could be in the scope of the definition for public administration entities in the NIS2 Directive. The most prominent media companies would be public broadcasting companies, that could fulfil the criteria of the definition for public administration entities if they are considered to have any public powers. There might not be many of these companies, but some do have potential. Yleisradio Oy could fulfil the criteria of public administration entity, as it is funded by tax money, does

---

[134] Case C-31/87 Beentjes v. Netherlands.
[135] See Joined Cases C-21/03 and C-34/03 Fabricom SA v Belgium.
[136] Case C-337/05 Commission v. Italy (Agusta and Agusta Bell Helicopters).

not have a commercial character,[137] has a legal personality as it is a limited liability company, and complies by public procurement legislation when purchasing goods and services.[138] Therefore Yleisradio Oy is most likely in the scope of the Directive, which consequently means that media companies can in some cases be included in the scope of NIS2 by the inclusion to this sector, along the possibility of being included in the digital infrastructure by the ownership of a public electronic communications network.

Different Member States have different public broadcasting company arrangements, and some are more tied with the function of society and the state, and some are at least partly funded by commercial activities, while others are funded almost exclusively by tax money. This makes it impossible to classify all public broadcasting companies or media companies under the public administration sector. An individual assessment has to carefully be made for each entity.

[137] Yleisradio, "Ylen talous."
[138] Yleisradio, "Hankinnat – näin Yle hankkii tavaroita ja palveluja."

4 Impact of the CER Directive and other factors affecting the scope of application of the NIS2 Directive

This chapter aims to include the ”additional” three interpretation methods discussed earlier. All three interpretation options are used; the intentions of the legislature, possible conflicts between internal or external legal texts and the legislation text, and the advantages and disadvantages of different interpretations and their consequences are taken into account in this chapter. The chapter will start with the impact of the CER Directive, the intentions of the legislator, and will then move to considering other factors affecting the analysis, and advantages and disadvantages of different interpretation options, as well as considering the impact of the differences between the individual media companies. The aim is to provide a recommendation, an informed opinion, for the interpretation of the scope of the Directive.

4.1 Impact of the CER Directive

As discussed earlier in this thesis, Article 2(3) of the NIS2 states that, “Regardless of their size, the Directive applies to entities identified as critical entities under Directive (EU) 2022/2557”, the CER Directive. This means that if a media company were to be identified as critical entity under the CER Directive, NIS2 Directive would apply to them, regardless of the size of the entity.

The CER Directive aims to function alongside the NIS2 Directive in matters that do not concern cybersecurity specifically, but the resilience of essential service providers, focusing on physical risks. Article 1(e) CER Directive states that the Directive “lays down measures with a view to achieving a high level of resilience of critical entities in order to ensure the provision of essential services within the Union and to improve the functioning of the internal market.”[139]

[139] The measures are set out in Articles 12–15 CER Directive. These include risk assessments which consider natural and man-made risks which could lead to an incident, resilience measures which are intended to account for the risks identified, including measures for prevention, responding, and recovering, much like those of NIS2’s cybersecurity measures. Critical entities must also, when reasonable and permitted, submit requests for background checks on personnel holding or in consideration for sensitive roles in or for the benefit of the critical entity, in particular in relation to the resilience of the entity, or on those in consideration for, or already authorised to directly or remotely access its premises, information or control systems.

Article 1(2) stipulates the relation to NIS2, and the implementation of both directives to Member States' national legislation:

> This Directive shall not apply to matters covered by Directive (EU) 2022/2555.... In light of the relationship between the physical security and cybersecurity of critical entities, Member States shall ensure that this Directive and Directive (EU) 2022/2555 are implemented in a coordinated manner.

The aim is to ensure that Member States implement strategies that provide a policy framework for a coordinated information sharing between the competent authorities under the CER and NIS2 Directives so that both cyber and non-cyber, risks, threats and incidents, and supervisory tasks can be accounted for in a well-coordinated manner.[140] In preamble (30) NIS2, it is stated that

> In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) 2022/2557 of the European Parliament and of the Council and this Directive. To achieve this, entities identified as critical entities under Directive (EU) 2022/2557 should be considered to be essential entities under this Directive (NIS2).
>
> ...Furthermore, in order to streamline supervisory activities between the competent authorities under this Directive and those under Directive (EU) 2022/2557 and in order to minimise the administrative burden for the entities concerned, those competent authorities should endeavour to harmonise incident notification templates and supervisory processes.

Entities could be in the scope of both Directives, as the definitions of entities concerned are very similar in both. Those that are likely to be in the scope of both the NIS2 and CER Directives, are in a position that could prove to be burdensome. This is why the EU legislator has accounted for this risk of duplication of obligations for those entities. In particular, the digital infrastructure sector has been identified by the EU legislator to be potential in being in the scopes of both Directive.[141] Preamble (20) stipulates that entities in this sector are exempt from some obligations of the CER Directive, as those obligations are equivalent to those set in NIS2. The preamble explicitly states that these entities should be identified as critical by Member States for both the CER and NIS2 Directives, as entities in digital infrastructure sector are very important for all other sectors stipulated by the CER Directive, which is

---

[140] Article 4(1)(g) CER and Article 7(1)(g) NIS2.
[141] Among banking and financial market infrastructure sectors. See Article 8 CER.

believable as digital infrastructure is increasingly important for the everyday functions of societies. The preamble also states that a higher level of resilience should be maintained for the digital infrastructure sector. It seems then that this sector is considered particularly important and is expected to maintain a higher level of resilience than perhaps the other sectors, and that the Union legislator expects Member States to identify this sector as being in the scope for both NIS and CER Directives. Perhaps a more vigilant attitude is expected on the identification of these entities.

Let's now have a look at the CER Directive and its definition of critical entities. In its article 2, point (1), a critical entity is defined as "a public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the sectors set out in the third column of the table in the Annex". The identification of critical entities is done by Member States, for entity types listed in the Annex, taking account national risk assessment and Member States' strategy stipulated in Articles 4 and 5 CER. In article 6(2), the following criteria is set for the entity to be identified as a critical entity:

> (a) the entity provides one or more essential services;
>
> (b) the entity operates, and its critical infrastructure is located, on the territory of that Member State; and
>
> (c) an incident would have significant disruptive effects, as determined in accordance with Article 7(1), on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors set out in the Annex that depend on that or those essential services.

Essential service is defined in Article 2(5) CER as a service crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment. Media companies could be vital for at least societal functions and public health and safety. If information cannot be distributed, public health could be endangered, if for example emergency warnings cannot be broadcasted on radio or tv channels. The media companies most likely to be brought within the scope of this Directive, if at all, would be larger companies and those with a public service mandate.

In the Annex of the CER Directive is a list of sectors, subsectors, and the third column mentioned above, categories of entities. The sectors are outlined in the annex of CER and include:

> Energy: Including electricity, district heating and cooling, oil, gas, and hydrogen.
>
> Transport: Including air, rail, water, road, and public transport.
>
> Banking: Including credit institutions.
>
> Financial market infrastructure: Including trading venues and central counterparties.
>
> Health: Including entities such as hospitals, laboratories, research and manufacturers of medical and pharmaceutical products and equipment.
>
> Drinking water: Including the supply and distribution of drinking water.
>
> Waste water: Including the collection and processing of wastewater.
>
> Digital infrastructure: Including internet exchange points, domain name service providers, data centre service providers, and cloud computing service providers, providers of content delivery networks, trust services, public electronic communications networks and electronic communications services.
>
> Public administration: Including public administration entities of central governments as defined by national law.
>
> Space: Including operators of ground-based infrastructure that support the provision of space-based services.
>
> Production, processing and distribution of food: Including food businesses.

Of those, most viable for a media company would be, based on the assessment done before for NIS2, digital infrastructure and public administration. The definitions of subsectors in the digital infrastructure sector refer to the definitions of the NIS2 Directive and as we already have taken a look at the definitions of the digital infrastructure sector in the NIS2 Directive, we can largely exclude this sector from applying to media companies in the context of the CER Directive, apart from companies that own the network used as discussed before. Individual assessment is yet again important here.

Let’s take a look at the sector of public administration. We have already stated that some media companies could be included in the NIS2 definition of public

administration. Article 2(10) of the CER Directive defines public administration entities as follows:

> 'public administration entity' means an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:
>
> (a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;
>
> (b) it has legal personality or is entitled by law to act on behalf of another entity with legal personality;
>
> (c) it is financed, for the most part, by the State authorities or by other central-level bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State authorities or by other central-level bodies governed by public law;
>
> (d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

The definition and conditions in question are similar for public administration entities, though not identical, as those in NIS2 Directive. In the definition of public administration entities of the CER Directive, regional authorities are excluded. The assessment done before in the previous chapter in the case of NIS2, indicates that media companies could be in the scope of application of the CER Directive. The assessment under Article 6(2) is the responsibility of the Member States. The author of this thesis is of the opinion that a clear majority of media companies, including public broadcasting companies, would be left out of the scope of CER Directive, on the basis of the assessment of Article 6, and by the fact that the physical resilience of media companies is not as essential to their functioning as cybersecurity. Media companies could operate virtually in any location, as the work for potentially essential services, those being distribution of emergency warnings and news production, could be done remote or in the cloud, at least to some extent. Media companies are not bound to a set physical location and do already have a substantial part of their work in the cloud, or are in the process of migrating to cloud, as for example Yleisradio stated in its annual report. Moreover, media companies could have geographically distributed locations for producing that essential service. Studio operations are usually centralised to a specific location, but the production of those

potentially essential services in permanent studios is likely not of paramount importance. The actual broadcasting, uploading and upkeeping of content is done through digital solutions, and the measures for resilience of these systems is left to those who run them.

Therefore, media companies may be considered to fall within the scope of the NIS2 Directive, in accordance with Article 2(3) NIS2, based on the assessment that there is a possibility for some media companies to be included in the scope of application of the CER Directive. However, this is unlikely in opinion of the author of this thesis.

If the company would fulfil the criteria for sectors of public administration entity or digital infrastructure in the NIS2 or CER Directive, the company could be included in the scope of both Directives. Final and binding decisions are done by the national legislators. Some ambiguity is left for the assessment of the scope of the Directives, but this is often the case in implementing directives. The individual media companies will have to make their own assessment and, in a metaphorical sense, take a side until further notice by national authorities.

4.2 Other factors influencing the scope of application of the NIS2 Directive

The analysis in this thesis has so far focused on the wording of the legislative text, which does have precedence in interpretation of legal texts. Following the modern approach on interpreting legal texts, we have to look at indications of different interpretations. What we can now do, is find other, non-governmental and non-official sources that indicate on this subject. This chapter contextual factors on the potential application of the NIS2 Directive to media companies.

Antonio Arcidiacono, Director of Technology and Innovation at the European Broadcasting Union (EBU) wrote in an article that people still need access to reliable and trustworthy information in times of crisis. EBU has 68 members representing 113 organisations in 56 countries. As stated by the Union, “Membership is for broadcasting organizations whose countries are within the European Broadcasting Area, as defined by the International Telecommunication Union, or are members of

the Council of Europe".[142] The European Broadcasting Area defined by the International Telecommunication Union ITU extends outside the commonly known geographical area of Europe, i.e. reaching countries of Saudi Arabia, Russia, Morocco, and Iceland.[143]

In the article, Arcidiacono explained that media is not included in the concerned sectors of NIS2, but that some countries are opting to include media companies in the scope of national regulations that are changed to implement the NIS2 Directive.[144] What can be concluded from this post is that the EBU's position is that some media companies are critical entities based on national legislation, and that the continuity of them must be safeguarded whether or not they are in the scope of the Directive. National legislation is what will determine regulation that concerns media companies based on NIS2. This is in line with the results of the analysis of this study. The EBU can be seen as an important institution in the area of European broadcasting activities and for its members. EBU describes itself as "the world's foremost alliance of public service media, representing over a hundred organizations worldwide. At the EBU, we strive to secure a sustainable future for public service media. We provide our Members with world-class content from news to sports and music, and build on our founding ethos of solidarity and co-operation to create a centre for learning and sharing."[145] EBU will therefore have to be given a certain amount of authority on the interpretation of the Directive, as it is an organisation with substantial expertise on the activities of public broadcasting companies. Articles such as these are not binding legal sources, but in this case, we can derive contextual support as we look for any opposing or supporting arguments on the question of the applicability of the Directive to media companies.

Media companies can have a role in the distribution of emergency warnings, as discussed before in this thesis. This alone has the potential to include them in the national scope of a critical entity, even if it is not worded as such in the Directive text. This would not by itself place them in the scope of the Directive, but clearly would

---

[142] European Broadcasting Union (EBU), "Our Members." EBU is not directly affiliated to the European Union. The details and nature of EBU members vary significantly, and these companies do not have a uniform function in the member countries, meaning that the function of these companies cannot be compared directly to each other.
[143] International Telecommunication Union ITU, "Radio Regulations," Article 5.14.
[144] Arcidiacono, "Can We Keep the Information Flowing?"
[145] EBU, "About the EBU."

confirm the critical role of such an entity. The Finnish government has recognised media and its infrastructure as an essential area of protection of society.[146] In addition to this, Laki Yleisradio Oy:stä, the act on Yleisradio Oy and Laki vaaratiedotteesta, the act on public emergency alerts include provisions that obligate Yleisradio as part of the public broadcasting mandate to transmit information provided by the authorities and to prepare for the operation of television and radio broadcasting in exceptional circumstances,[147] and that the process is the following;

> The competent authority sends a hazard report to the Emergency Response Centre, after which, The Emergency Response Centre transmits the incident report to the telecommunications terminal application and to Yleisradio Oy for distribution on radio and television.[148]

Yleisradio has an integral part of the process in which these emergency warnings are broadcasted. Same obligations are also given to other media companies. Laki sähköisen viestinnän palveluista 7.11.2014/917 (Act on electronic communications services) states that

> Public communications networks and services and the communications networks and services connected to them must be designed, built and maintained in such a way that: 14) they operate as reliably as possible even in emergency situations as referred to in the Emergency Preparedness Act (1552/2011) and in situations of disruption of normal; 15) hazard information issued by the authorities can be communicated to the public in accordance with specific provisions;[149]

and that

> A telecommunications undertaking and a holder of a licence to operate a radio service … are obliged to provide the public without delay with a hazard communication, the provision of which is regulated by the laki vaaratiedotteesta (466/2012, Hazard Communication Act) …
>
> The operator … must ensure that the hazard communication can also be transmitted in the event of normal disruptions and in emergency situations as referred to in the valmiuslaki (Emergency Preparedness Act).

---

[146] Valtioneuvoston päätös huoltovarmuuden tavoitteista 1048/2018. The Finnish language has the term “huoltovarmuus” which translates best to security of supply or emergency supply. A quick web search shows that the term security of supply is used mostly in matters concerning the supply of electricity. Huoltovarmuus is a broader term that expands to all critical functions of society, including at least food, health care, electricity, water, and financial services. For more information, see https://www.huoltovarmuuskeskus.fi/en.
[147] Laki Yleisradio Oy:stä 7 § 2 mom. 7 kohta.
[148] Laki Vaaratiedotteesta 7 §.
[149] Laki Vaaratiedotteesta 243 § 1 mom. Point 14 and 15.

> The operator shall also participate in the regular testing of the hazard communication system on the initiative of the authority.[150]

These provisions in Finnish legislation show that media companies, in particular television and radio operators do have an obligation to continue functioning under exceptional situations and situations of emergency. This underlines the importance of these entities for society and indicates that they have an integral part of the emergency warning system in Finland. Finland undoubtedly differs from other Member States in some respects on the organisation of society and the role and perceived trustworthiness of the media.[151] This could have an impact on the scope of application of the Directive. Attitudes towards media and its role in society, and the need for reliable information vary between Member States. Further societal analysis is left outside of the scope of this thesis.

The sector production, processing and distribution of food in NIS2 is defined to include "any undertaking, whether for profit or not and whether public or private, carrying out any of the activities related to any stage of production, processing and distribution of food, and which are engaged in wholesale distribution and industrial production and processing" by the Union legislator.[152] Considering that under the implementation measures following the NIS1, Germany defined that the scope of the food sector covers those that pass a threshold of at least 434.500 tons of food or 350 million litres of beverages annually produced,[153] this shows clearly that the definition of NIS2 for this sector is considerably wider than in NIS1, as there are no thresholds of production volume. The significant increase in the number of entities included in the scope of the Directive indicates a significant enlargement of the scope. If other sectors are to be defined as broadly, as for example the food business sector, the author does not see any reason not to include media companies closely affiliated with

---

[150] Laki Vaaratiedotteesta 279 § 1 and 2 mom.
[151] Reuters Institute's Digital News Report 2024 found that respondents in Finland have the highest level of trust in news of all 47 countries surveyed, 69 percent of respondents in Finland trust most news most of the time. Finland is an outlier in this regard. Report available here: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf.
[152] Annex II NIS2 refers to the definition of Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council.
[153] Annex 3 part 3 no. 1.1.1 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz.

member state governments in the public administration sector of the NIS2. The inclusion would also, in the author's view, serve the purpose of the Directive.

The inclusion of media companies at least to the list of important entities is further underlined by the nature of these companies, which is largely similar to for example postal services, which are explicitly included in the scope. It could be argued that informing people in possible emergency situations is vital to the functioning of society, in similar ways as postal services. If something of an emergency nature were to happen, media services are undoubtedly a critical service for the best possible well-being of people. Media companies which, depending on the specifics of a Member State, are more or less officially obliged to inform the public and provide news, particularly in emergencies, could be included in the scope of the Directive. This will be solved by the member countries themselves, possibly in cooperation with the entities in question. Yleisradio was heard by the Finnish Parliament on the implementation of the NIS2, which strongly suggests the company could be considered to be included in the scope of the proposed legislation.[154] Member States could also interpret the Directive more broadly if they consider the media company's role significant enough to be considered critical.

The minimum harmonisation requirement can be interpreted as a signal for the inclusion of media companies in the scope. If a member state believes a media company is critical to the functioning of society, it can choose to include it in the scope of the national legislation. It can be concluded that ultimately, the classification of a broadcasting company, or any entity on that matter, depends on the national implementation and interpretation of the Directive text done by national legislators. This somewhat goes against the intention of the legislator, in that the goal of the Directive is to level out the differences in implementation. This could act as a counterargument on including media companies to the scope of application of the Directive. On the other hand, this argument is not particularly strong, as there are significant differences in the operational environments of European media companies, that justify a different and varying interpretation between Member States.

---

[154] Unfortunately, the documents for the expert opinions submitted by Yleisradio are not available at the Eduskunta website. If they at some point are uploaded to the website, the URL to where they can found is https://www.eduskunta.fi/FI/vaski/KokousPoytakirja/Sivut/LiVP_45+2024.aspx.

4.3 Review of national interpretations

This chapter will gather some information on different implementation measures Member States have proposed or already done. This review is not meant to be a comprehensive review, but a brief look into a few Member States' implementation measures, with a focus on the implementation of the public administration sector of NIS2, using public broadcasting companies of those Member States as examples. So far, at the time of writing this thesis, by September 2024, two Member States have implemented the NIS2 Directive. These are the Kingdom of Belgium and the Republic of Croatia.[155] In addition to these, this chapter will review measures taken by Finland, which are currently in the legislative process. There is a possibility for translation errors as the legislation texts were translated into English using translation tools.[156] The broad picture was relatively reliably captured.

Belgian law has three conditions for an entity to be defined as public administration; 1. it should not have an industrial or commercial character; 2. it does not primarily carry out an activity listed in the type of entity column of another sector or sub-sector of one of the annexes to the law (same sectors as in the NIS2 Annex) and 3.it is not a legal person governed by private law.[157] It seems that the Belgian legislator has combined the criteria (c) and (d) of Article 6(35) NIS2, and does not explicitly say anything on the financing of the entity. Entities that are governed by private law are excluded. This would exclude limited liability companies, such as Yleisradio Oy (at least in the majority of governance matters, excluding public procurement) if it were Belgian, from the scope of the national legislation.[158] Belgium's public broadcasting companies De Vlaamse Radio- en Televisieomroeporganisatie (VRT), Belgisches Rundfunk- und Fernsehzentrum Sendungen in Deutscher Sprache (BRF), Télévision belge de la Communauté culturelle francaise (RTBF) are public limited companies

---

[155] National transpositions by Member State as of 16.09.2024.
[156] Google Translate embedded into Google Chrome, Sanakirja.fi, and DeepL Translate. Google Lens was also used to help translate the Croatian cybersecurity law's Annexes. The possibility of translation errors cannot be completely ruled out. These translation services use artificial intelligence.
[157] Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique 34°.
[158] Provisions on jurisdiction and territoriality are in Article 26 NIS2, which (26)(1)(c)) provides that "Entities falling within the scope of this Directive shall be considered to fall under the jurisdiction of the Member State in which they are established, except in the case of;...public administration entities, which shall be considered to fall under the jurisdiction of the Member State which established them."

and/or public institutes.[159] This would suggest that these companies could be in the scope of the Directive and national legislation.

Croatia's law on cybersecurity, which implements the NIS2 Directive,[160] states that public administration entities are sub-sectored into bodies of state administration, other state bodies and legal entities with public powers, private and public entities that manage, develop or maintain the state information infrastructure in accordance with the law regulating the state information infrastructure, and units of local and regional self-government.[161] Croatia has one public broadcasting company, Hrvatska radiotelevizija (HRT). HRT is a public institution. It is regulated by national legislation, similar to Yleisradio Oy in Finland.[162] HRT states that it is free of any commercial interest[163], but also has some commercial revenues that finances its activities.[164] The company also publishes public procurement details on its websites, which suggests that the company is subject to regulation on public procurement.[165] This means that HRT could well be in the scope of the Directive.

Finland has decided to implement the Directive into different laws, but also proposes a new law, the cybersecurity law.[166] Public administration entities would be included into the scope of Laki julkisen hallinnon tiedonhallinnasta, the Public Administration Information Management Act,[167] which would concern the cybersecurity matters of public administration, along other information security matters it already stipulates. This law states that a critical entity is an entity identified as a critical entity under the Article 2(1) CER Directive, which in this case means that the entity is a critical entity if the member state in question has identified the entity as a public administration entity in its national legislation. The law on Yleisradio Oy states that Yleisradio is a public service company, that operates within the administrative sphere of the Ministry of Transport and Communications.[168] This indicates that Yleisradio Oy

---

[159] Crossroads Bank for Enterprises, "Public Search."
[160] Zakon o kibernetičkoj sigurnosti.
[161] Zakon o kibernetičkoj sigurnosti, PRILOG I. SEKTORI VISOKE KRITIČNOSTI.
[162] Zakon o Hrvatskoj radioteleviziji.
[163] HRT, "O HRT-u."
[164] Zakon o Hrvatskoj radioteleviziji Članak 33.
[165] HRT, "Javna nabava."
[166] Kyberturvallisuuslaki, which was proposed in the proposal HE 57/2024 vp. Available only in Finnish.
[167] Laki julkisen hallinnon tiedonhallinnasta, 906/2019.
[168] Laki Yleisradiosta 1 §, Here translated into English.

would most likely be included in the scope of the Directive, and the national law.[169] When considered together with the analysis made in chapter 3 of this thesis, it is very likely that Yleisradio Oy is in the scope of the Directive, and should also be in the scope of national law.

National legislator has some freedom in considering the implementation measures for NIS2, as can be seen with the differences in the definitions of public administration entities in the three examples observed above. The specific criteria for the definition of public administration entity are set by the national legislator. This is expected, as directives are meant to be implemented in a way that integrates well into the national legislation framework. National legislation, arrangements regarding emergency warnings and the arrangements for the security of supply of the Member State, the role of public broadcasting and other media companies and their relation to State all affect the end result. Ultimately, the national definitions and criteria for the NIS2 sectors influences if media companies are subject to NIS2 cybersecurity obligations. Those obligations of NIS2 are implemented into national legislation, and those obligations are followed in the manner explained in the national legislations.

It can be concluded that the implementing measures are important, as is careful preparation of the wording of legislative text. Directives are a great tool in bringing harmonisation to Member States' legislation in a not-so-intrusive way as regulations would. The upside of directives is that they can be implemented in a way that works best for the individual legislation framework of a member state. As analysed, there are already differences between these three cases of national implementation. This can generate differences between the scope of national legislations between Member States. This should be avoided as far as possible to uphold the intent of the legislature. The European broadcasters, and other media companies, could be in contact with other broadcasters through the EBU to discuss the obligations imposed by the new legislation, and the cybersecurity measures that are to be updated, despite the possible differing interpretations of the Member States on the scope of application of the Directive and its implications on media companies and state-owned public broadcasting companies. Member States will always make

[169] Specifically Laki julkisen hallinnon tiedonhallinnasta.

compromising decisions when implementing directives, but this specifically what the CJEU is intended to make rulings on.

5 Risk-management measures required by the NIS2 Directive

This chapter addresses the question of what the Directive requires media organisations to do when they fall within the scope of the Directive due to their individual characteristics or due to national implementation decisions. This chapter will provide a part of the answer the supplementary research question of this thesis; *What is the impact of the Directive on media companies operating within the Union?*

NIS2 sets out a list of ten different cybersecurity risk-management measures for essential and important entities, along supervisory and enforcement measures, which are meant to ensure compliance with the legislation. The Directive distinguishes between essential and important entities for the purposes of different supervisory and enforcement measures. Essential entities are subject to ex ante supervision, while important entities are subject to ex post supervision. This has also been referred to as "fully-fledged" and "light supervisory regimes" by the legislator.[170]

Let's start by defining whether media companies are important or essential entities. This is done to narrow down the set of obligations for media companies given in the Directive. Article 3 sets out conditions for entities to be identified as essential.[171]

> (a) entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC;
>
> (b) qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;
>
> (c) providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC;
>
> (d) public administration entities referred to in Article 2(2), point (f)(i);
>
> (e) any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e);

---

[170] Preamble (70) NIS2.
[171] Article 3(2) NIS2 states those which do not qualify as essential entities pursuant to paragraph 1 of the Article shall be considered important entities.

> (f) entities identified as critical entities under Directive (EU) 2022/2557, referred to in Article 2(3) of this Directive;
>
> (g) if the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148[172] or national law.

Based on the assessment conducted earlier in this thesis, media companies could be considered as essential entities on criteria (a),[173] (c),[174] (d),[175] (e), and (f). Criterion (g) does not apply, as media companies were not in the scope of NIS1. Therefore, media companies would be identified as essential entities if they were included in the public administration entity or digital infrastructure sectors. The supervisory and enforcement measures in relation to important entities are not discussed further in this thesis. These measures are provided for in Article 33 and are largely similar to those in relation to essential entities. Differences lie in the frequency and intensity of the measures.

Both essential and important entities have the same cybersecurity risk-management measures set out in Article 21(2) NIS2, which are the following:

> (a) policies on risk analysis and information system security;
>
> (b) incident handling;
>
> (c) business continuity, such as backup management and disaster recovery, and crisis management;
>
> (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
>
> (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
>
> (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
>
> (g) basic cyber hygiene practices and cybersecurity training;

---

[172] Those identified as essential in NIS1.
[173] Annex 1 had sectors digital infrastructure and public administration, which could include media companies.
[174] If the media company would own the network used, or if they do not have editorial control over, or do not provide the content transmitted.
[175] If defined in national law as a part of central government.

> (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
>
> (i) human resources security, access control policies and asset management;
>
> (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

These measures align with the previously mentioned six-step, Classic or the PICERL model of incident response, and each measure goes into one of those steps. Majority of these measures are designed to prevent incidents. The measures are relatively common and already widely used by organisations. This demonstrates the fundamental nature of the Directive; the objective is to require all entities subject to the Directive to implement cybersecurity measures that are aligned with current standards. Member States must implement these measures and ensure that they are implemented correctly by entities, as stated in Article 21(1) and (2):

> 1. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.
>
> 2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents…

The first paragraph demonstrates clearly that the use of widely recognised standards is considered ideal by the Union legislator. Additionally, it indicates that a certain degree of flexibility is permitted with regard to the implementation of the measures for the entities in question. Entities can adapt their cybersecurity measures in a manner that is proportional to the activities in which they engage and the nature of their business activities, in accordance with the principle of proportionality, taking into account the entity's risk exposure, entity's size and the likelihood of incidents, and their severity including their societal and economic impact, as well as cost of implementing the measures. At the same time entities are expected to keep the

measures up to state-of-the art standards. This assessment requires a considerable amount of resources from organisations.[176]

The "all-hazards approach" means the attitude towards possible risks on the physical environment of the network and information systems "from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, an essential or important entity's information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. The cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena, in line with European and international standards, such as those included in the ISO/IEC 27000 series. In that regard, essential and important entities should, as part of their cybersecurity risk-management measures, also address human resources security and have in place appropriate access control policies. Those measures should be consistent with Directive (EU) 2022/2557."[177]

When implementing measures for supply chain security, provided in Article 2(2)(d), "entities (should) take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures." This introduces an additional requirement for businesses, which in practice is an obligation to include cybersecurity terms into supplier contracts. Preamble (85) of the Directive states that

> essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those

---

[176] In the proposal for the Finnish implementation measure HE57/2024, estimates for the number of man-years and the cost of the risk-management measures were provided. The total cost of the activities is in the hundreds of thousands of euros. The estimates are from a survey done in the production, processing and distribution of food and manufacturing sectors, and there were 20 participating companies. The report is available here, only in Finnish: https://api.hankeikkuna.fi/asiakirjat/34beb41e-515a-4fcd-a824-5136fd497329/310cde7e-950a-43f3-8429-2340a5d525b9/KIRJE_20230614065803.PDF.

[177] Preamble (79) NIS2. In this text we can see a reference to the ISO/IEC 27000 series, which demonstrates the attitude and considerable respect towards widely used standards in the field of cybersecurity by the Union legislator.

entities could consider risks stemming from other levels of suppliers and service providers.

These measures are aimed to enhance the security of the supplier's operations, and the products supplied. Additionally, this imposes an obligation on businesses to ensure that their suppliers' suppliers have implemented effective cybersecurity measures. This could prove burdensome and expensive for a considerable number of entities. Also, the entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) NIS2, which sets out the process by which the Cooperation Group,[178] in collaboration with the Commission and ENISA, may conduct assessments of specific critical ICT services, systems, or product supply chains, considering both technical and non-technical risk factors.

5.1 Reporting obligations (Article 23)

Article 23 sets out the reporting obligations for essential and important entities. This chapter explains when a report must be made, for whom, and what information it should contain.

When an incident is concerned significant, the entities shall notify the member state's Computer security incident response team(s) or CSIRT(s),[179] or a competent authority when applicable, as per Article 23(1) "without undue delay the recipients of their services of significant incidents that are likely to adversely affect the provision of those services." This notification has to include as per Article 23(2) "any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself."

An incident is concerned significant if that incident has a significant impact on the provision of an entity's' services as per paragraph 3:

---

[178] See Article 14 NIS2. In short, Cooperation Group supports and facilitates strategic cooperation and the exchange of information among Member States.
[179] Article 10(1) NIS2 states that Each Member State shall designate or establish one or more CSIRTs. CSIRTs have tasks regarding, inter alia, monitoring, analysing and responding to vulnerabilities and incidents at national level and assisting entities. All tasks are listed in Article 11(3) NIS2.

> An incident shall be considered to be significant if:
>
> (a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
>
> (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

The timeline and content of the notifications is stated in paragraph 4:

> (a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;[180]
>
> (b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;
>
> (c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;
>
> (d) a final report not later than one month after the submission of the incident notification under point (b), including the following:
>
> (i) a detailed description of the incident, including its severity and impact;
>
> (ii) the type of threat or root cause that is likely to have triggered the incident;
>
> (iii) applied and ongoing mitigation measures;
>
> (iv) where applicable, the cross-border impact of the incident;
>
> (e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

As stated in paragraph 5; after the early warning, the CSIRT or the competent authority has to provide a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational

---

[180] As Article 23(1) NIS2 states: The information provided has to help the CSIRT or competent authority to determine any cross-border impact of the incident.

advice on the implementation of possible mitigation measures or guidance on reporting the significant incident to law enforcement authorities in case of the incident being of criminal nature, and technical guidance if the entity so requests. As expressed in detail in paragraphs 6–11 , the CSIRT or competent authority will process the notification further, also to ENISA and The Cooperation Group, and contact the entity if its actions are required later in the informing of the public on the incident.

The 24-hour incident reporting timeline is a significant addition to the requirement of the NIS1's "without undue delay"[181] – and the GDPR's 72-hour requirement in case of a personal data breach,[182] that are often combined with cyberattacks. The obligation for the 24-hour early warning and later reporting could cause difficulties for smaller entities. These entities will not always have the resources to assess the incident in time for the warning and will have to use external consultants. This makes the time window very challenging. The same resources and time could be used to assess the actual incident and its damages.[183] This will undoubtedly increase the workload and resource needs for organisations, but it will also help to ensure rapid response and limit further damage. The early warning time window of 24 hours is welcome in ensuring a swift development of incident handling measures and will facilitate the co-operation between CSIRTS, authorities and the entity under attack. It will also help in ensuring that organisations are ready to act if an incident were to occur.

The threshold for reporting has been criticised for being vague. There is possible ambiguity in the determining if a threat is significant. One attempt at defining a guideline for determining the threshold of reporting has been done by Schmitz-Berndt, although the wording of the Directive is quite clear on that reporting must be made if the threat is capable of causing considerable material or non-material damage or severe operational disruption or financial loss for the entity concerned.[184] This indicates that there is room for interpretation on the reporting threshold and that the entities have to figure out themselves when a report must be made. In

---

[181] Article 14 NIS1.
[182] Article 33 GDPR.
[183] Philipp Eckhardt, "NIS2 Directive: New EU Rules on Cybersecurity," 13.
[184] See Schmitz-Berndt, "Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS2 Directive."

practice, entities could be in contact with the authorities regarding the assessment of the reporting thresholds, but this will also further add to the workload of both the entities and authorities. Voluntary reports can also be recommended in cases where the entity is not certain if a report must be made or not. In paragraph 1 it is assured that “the mere act of notification shall not subject the notifying entity to increased liability.” Therefore, entities can, in principle, give voluntary notifications without fear of incurring greater liability.

Ensuring a process for voluntary notifications and information sharing between entities themselves using their networks, and between entities and competent authorities along the lines of Articles 29 and 30 is expected from Member States. Entities falling out of the scope of the Directive should also be able to exchange information on a voluntary basis.

5.2 Certification and standardisation (Articles 24 and 25)

Article 24 provides that Member States may require critical sectors to use certified ICT products, ICT services and ICT processes to ensure high standards of cybersecurity. This certification, based on schemes developed under the EU Cybersecurity Act, is designed to help standardising cybersecurity across critical sectors. The Commission can adopt delegated acts on which categories of entities must use certain certified technologies, especially when cybersecurity problems are identified. If an appropriate certification scheme does not exist, ENISA may be asked to develop one. This seems to mean that entities might have to use technologies that are approved to be used in the EU and will have to transfer their systems to be used within the approved ecosystems, if the Member State so decides. This sounds quite intrusive, but what will happen is yet to be seen.

Article 25 promotes the use of European and international cybersecurity standards to harmonise practices across the EU:

> 1. In order to promote the convergent implementation of Article 21(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.

> 2. ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered.

This in turn introduces more costs and an increased workload for those affected. But on the other hand, these measures will, in principle, help in adopting secure technologies and complying with international and European standards, thereby contributing to the resilience of the Union entities' critical infrastructure. The actual implementation of these articles will be left to the Member States, and that will be an interesting development to follow.

5.3 Supervisory measures, enforcement, and fines (Articles 32 and 34)

Article 32 lays down the supervisory and enforcement measures that essential entities are subject to. As said before, the measures are *ex ante* inspections. This means that the competent authorities have the power, as stated in Article 32, at least for:

> (a) on-site inspections and off-site supervision, including random checks conducted by trained professionals;
>
> (b) regular and targeted security audits carried out by an independent body or a competent authority;
>
> (c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity;
>
> (d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;
>
> (e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;
>
> (f) requests to access data, documents and information necessary to carry out their supervisory tasks;
>
> (g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The enforcement measures to make sure that the entities comply with the implemented legislation are the following, stated in paragraph 4:

> (a) issue warnings about infringements of this Directive by the entities concerned;
>
> (b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive;
>
> (c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;
>
> (d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;
>
> (e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;
>
> (f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;
>
> (g) designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23;
>
> (h) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;
>
> (i) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.

As stated in paragraph 5; If these measures are not effective, even after giving a deadline by which the essential entity is requested to take the necessary action to remedy the deficiencies or to comply with the requirements of those authorities, the competent authorities have the power to:

> (a) suspend temporarily, or request a certification or authorisation body, or a court or tribunal, in accordance with national law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity;

> (b) request that the relevant bodies, courts or tribunals, in accordance with national law, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity.

Here is notable the liability of members of management of the entity in question. For chief executive officers this means that they have a larger incentive to make sure that their organisation complies with the requirements of the Directive. However, this does not apply to public administration entities per the final sentence of paragraph 5. As regards public administration entities, the liability of natural persons for breaches of their duties, which must be ensured by Member States according to paragraph 6, is without prejudice to national law.

Therefore, media companies that are considered public administration entities in the Directive, the liability and accountability of individual persons within those entities will be governed by national law, allowing Member States to determine the extent and nature of personal liability within the framework established by their national legal systems.

Article 34 sets out the conditions for imposing administrative fines on entities in cases of infringements of Articles 21 or 23. Fines must be effective, proportionate and dissuasive and take individual circumstances into account for each case. The Directive allows for significant fines to be imposed on companies that fail to comply with those Articles. Essential entities are subject to fines of a maximum of at least EUR 10 million or 2 percent of their total annual worldwide turnover, whichever is higher, for breaches of key provisions such as those set out in Articles 21 and 23. Important entities are subject to slightly lower fines of a maximum of at least EUR 7 million or 1.4 percent of their total worldwide annual turnover, whichever is higher. These fines are in addition to the measures referred to in Article 32(4) points (a) and (h) and 32(5), ensuring that non-compliance carries significant consequences.

5.4 Sectoral legislation (Article 4)

NIS2 could be considered as the new core legislation in the EU Cybersecurity legal framework, and could be seen as *lex generalis*, and the more sector-specific

legislation as *lex specialis*. For example, in the financial sector, it could be argued that the Regulation on digital operation resilience for the financial sector (DORA)[185] will be a *lex specialis* in relation to NIS2.[186]

In Article 4 NIS2, it is stated that

> Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities.

To assess if there is any sectoral legislation for media companies that meets the requirements of Article 4, let's have a look at EU law specifically on the security of media companies, part of what was already assessed in Chapter 2.3. The Audiovisual Media Services Directive applies to media companies and obligates the Member States to ensure that audiovisual media services do not endanger health and safety,[187] which could be, if interpreted broadly, understood to include also cybersecurity in matters that could endanger health and safety, but certainly not in the effect of the NIS2. The GDPR includes aspects of data security, but concerns personal data, not specifically cybersecurity in the effect of the NIS2 Directive. The ePrivacy is about privacy, not cybersecurity. No other legislation could be interpreted to consider cybersecurity specifically for media companies.

There is no sector-specific Union regulation concerning media companies that would meet the requirements of Article 4 NIS2 Directive. The first of these requirements is that the risk management measures are at least equivalent in effect to those laid down in Article 21(1) and (2). The measures of the Union legislation observed are not as effective as those in the NIS2 Directive in the field of cybersecurity, as those measures are very general in their nature.

Certain ambiguity can be seen in the phrasing of "at least equivalent in effect to the obligations laid down in this Directive". The phrasing is clarified in the preamble, but

---

[185] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.
[186] Vandezande, "Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor," 3.
[187] Audiovisual Media Services Directive Article 9(1)(c)(i).

this still leaves some room for interpretation and causes difficulties for entities in certain fields.[188] For example, concerns have been raised on the compatibility and interplay of the NIS2 and the Regulation on medical devices,[189] which have different notification requirements for manufacturers of medical devices in case of incidents.[190] Ambiguities like this are not a welcome sign and should be averted or at least quickly reacted to. However, there might be a reason for certain ambiguity. In preamble (22) the legislators' logic is explained; sector-specific Union legal acts are more likely to consider the specificities and complexities of the sectors concerned. This means that the Directive would potentially not take these factors into account as effectively as the sector-specific legislation. The introduction of legislation that is too specific would have the effect of hindering the possibility of implementing the measures on a wide range of entities.

These cybersecurity measures introduced in the Directive are nothing revolutionary or ground-breaking, but rather of a very basic level of cybersecurity measures any larger company should already have. What follows is the possibility of the Directive being a somewhat redundant regulation in that it will not elevate the quality of cybersecurity measures in the Union, but rather bring more entities into the scope of obligated measures, and consequently bring more entities to a basic level of cybersecurity, which is a positive development. The next chapter will further dive into the shortcomings and critique towards the Directive and the decisions made by the Union legislator.

---

[188] More on the difficulties of sectoral legislation and Article 4 NIS2 regarding manufacturers of medical devices: Biasin, and Kamenjašević, "Cybersecurity of medical devices: new challenges arising from the AI Act and NIS2 Directive proposals."
[189] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.
[190] Biasin and Kamenjašević, 168–171.

6 On measures to harmonise cybersecurity risk preparedness in the Union – Is the Directive destined to fail?

No legislation is perfect. There will always be demands for clarification on what the legislator has intended. A thorough assessment by actors other than the legislator will lead to questions and criticism. The measures that entities are required to implement in accordance with the Directive give rise to a number of questions, which must be addressed in order to ensure compliance. Is conforming to international standards enough? What is the actual level of quality of the measures that must be taken in order to comply? How extensive should the measures be?

Organisations are now deciding, or rather should have already decided, whether or not they are covered by the Directive. A stakeholder event held by the Finnish Ministry of Transport and Communications made evident that organisations are unsure on whether the Directive concerns their organisation or not,[191] and a quick online search also shows that there is a need for individual assessing whether this new legislation affects the functions of any given organisation. This assessment can be complex, as the analysis in this thesis proves. The change in the identification process for critical entities poses challenges for various organisations, but also for the supervising authorities, and may require considerable resources from both.

As management bodies are personally responsible for the adopted measures, they will want adequate documentation of the measures. In this regard, the requirement for documentation is one thing that needs further guidelines, if the supervision is in practice as extensive as proposed. The actual level of supervision done by national authorities will be observed later, but organisations will not want to take huge risks in this respect. On the other hand, the objective of minimum harmonisation could point to the road of less guidelines by the Commission. Some Commission guidelines on the application of specific Articles of the Directive have however been published already in 2023.[192] These were not guiding on the risk-management measures themselves but concerned scope of application of certain Articles of the Directive. More guidelines are expected to come, and this is a positive direction.

---

[191] Recording available at https://www.youtube.com/watch?v=lZWTbRxULks. English subtitles available.
[192] Guidelines on the application of Article 4(1) and (2) and Article 3(4) of the NIS2 Directive.

Guidelines could for example be provided for the use of AI in Cybersecurity, although it really is not the most pressing issue. NIS2 encourages the use of Artificial Intelligence along other innovative technology to improve cybersecurity capabilities, and detection and prevention of cyberattacks.[193] The usage of AI should comply with Union data protection law, among other legislation, and as preamble (89) states: "entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems." This ties into the Artificial Intelligence Act, which stipulates the security of those AI systems. Other issues, such as the trustworthiness of systems, trade secrets, the possibility for the technology of being used for illegal activities, and the apparent "hallucination" of facts that large language models can currently be accused of, should also be taken into account, but are not explicitly mentioned in the Directive. Usage of AI for incident handling and prevention should be considered, but the decision should not be done lightly and too eagerly, and extensive testing should always be conducted.

There are more fundamental problems than the usage of AI and its problems that are prevalent in the current discourse on the NIS2. The supervisory authorities responsible for the *ex post* and *ex ante* supervision of essential and important entities are in risk of becoming overburdened by the vastly increased workload. If the estimate of 160 000 entities affected by the Directive is true, this would mean that each Member State would have approximately 6000 entities in the scope of the new legislation, and when taking into account the inevitable differences in implementation and interpretation of the Directive, this number would not be divided evenly between the Member States, which consequently will bring differences in the impact of the Directive between the Member States. The number of entities has been criticised as being too high, and there could have been better alternatives, than the size of the entity, for distinguishing between the entities in and out of the scope, which would better consider the actual cybersecurity risks an entity has. These could also have had a role in determining the scope in tandem with the size of an entity. For example, the number of customers the entity has could have been a good addition to

[193] Preambles (51) and (89) of the NIS2 Directive.

the criterion.[194] However, there does not seem to be a perfect answer to this question, as having more criteria for evaluation would make the evaluation more complex.

The effectiveness of the actual measures has been questioned by Ferguson. Ferguson accuses the Directive of focusing too much on limiting the impact of attacks rather than preventing them in the first place. The measures of the Directive are accused of being not as effective as need be in the early phases of cyberattacks. Ferguson states that an attacker could progress through the reconnaissance phase of an attack with little interference if an organisation operates solely on the basis of the risk-management measures of the Directive.[195] By the time their presence is detected, attacker may have established an "entrenched and agile position" within the network and information system. If this criticism were to materialise, the future of the Directive would be at stake, and a review or even a revision would be inevitable. The lacking measures that need be brought to the legislation in opinion of Ferguson are the following: reconnaissance footprint assessment, vulnerability scanning of internal resources, penetration testing, reviews of internal and external threat intelligence, and modelling of threats.[196] These measures have a proactive attitude towards incident handling and more specifically, prevention, which seems to be lacking in the measured required by the Directive. The implementation of these measures could be provided for in future legislations or supplementing acts.

Non-governmental organisations provide frameworks for organisations looking for effective cybersecurity. It is widely accepted that international standards provide an excellent starting point for compliance with NIS2. The ISO/IEC standard families 27000,[197] 31000,[198] and 22300[199] are widely in use,[200] and offer clear guidelines for entities on information security, risk management and continuity issues. Some areas in these standards are very similar, and some are different to those in the NIS2 Directive. For example, both require risk assessments and management, regular

---

[194] Philipp Eckhardt, "NIS2 Directive: New EU Rules on Cybersecurity," 12.
[195] The reconnaissance phase is when the attack is being planned by the attacker, as the name suggests.
[196] Ferguson, "The outcome efficacy of the entity risk management requirements of the NIS2 Directive." 384.
[197] ISO/IEC 27000 is a popular standard family on information security management. Read more at.
[198] This standard family concerns risk management issues. Read more at https://www.iso.org/iso-31000-risk-management.html.
[199] ISO 22300 is a standard on Security and resilience. Read more at https://www.iso.org/standard/77008.html.
[200] ISO is a network of 169 national standards bodies, with over 25 000 international standards and standards-type documents published. Read more at https://www.iso.org/iso-in-figures.html.

reviews and updates and the obligation to abide by law.[201] A clear difference seems to be that NIS2 demands an early warning in 24 hours from when the incident was noticed and ISO/IEC 27001 and 27002 require a 72-hour notification.[202] There is a clear need for alignment of the measures of these standards and the new legislation. Multiple preambles[203] and Article 25 of the NIS2 explicitly refer to the ISO/IEC Standards or European and international standards as best practices that are to be promoted. These have clear potential to be recommended by the Commission in the future as the standards to be followed. Preamble (79) of the NIS2 refers to the ISO/IEC 27000 series as a baseline for addressing also the physical and environmental security of network and information systems. This series could be an ideal starting point for addressing the new measures needed, as they are already extensive and do provide for evidence that the organisation has taken a step towards comprehensive cybersecurity that is more or less in line with the NIS2.[204] Same could most probably also be said of the other standard families mentioned above.

But another question arises; if international standards are widely in use, respected, and recognised by customers, and the standards meet the overarching majority of the obligated measures of the NIS2, is there really a need for such a legislation? Is there a risk that the Directive will become redundant in terms of the risk-management measures it requires?

Legislation is an effective way to introduce measures to entities that do not already have them in place. Same applies to the NIS2 and its cybersecurity measures. The legislation does not bring a major change to the actual measures for organisations that already have industry standard cybersecurity measures in place. The requirement for a 24-hour early warning within becoming aware of a significant incident is a new requirement and the encouragement for information sharing is a positive development, but nothing fundamental is changed in the standard

---

[201] Kahmen, "The Relationship Between NIS2 and ISO 27001." A publication on the website of cybersecurity consultancy Turingpoint.
[202] Plasman, "Is ISO 27001 enough for NIS2 compliance?" A publication on the website of Ceeyu, a Cybersecurity SaaS platform provider.
[203] Preambles (58), (59), (79), (80), (81), and (99) NIS2.
[204] Harper, "NIS2: What The Proposed Changes Mean For Your Business." A post on the website of ISMS. ISMS is an organisation helping companies manage their information security: The author is of the opinion that a standard-based approach could be a "powerful first step" for organisations that want to achieve compliance with NIS2, and among having ISO 27001 in use, adding ISO 22301 would further "demonstrate compliance with NIS2". An approach like this could well be a good starting point, especially in a cost-effectiveness standpoint.

cybersecurity measures organisations have in place. But the point seems to be that it is not the purpose of the Directive to revolutionise cybersecurity. The purpose is to bring the measures to an adequate level in critical organisations in all European Union Member States, and not to have weak points in any critical entity in the Union. The author of this thesis is of the opinion that this is an ideal way to go forward with Union cybersecurity developments. The harmonisation measures are meant to ensure that there are no critical entities with lesser-than-standard measures in place. If an entity wants to take more extensive measures, it is free to do so. The idea is to elevate the bottom level of cybersecurity of critical entities to an appropriate level, which seems very reasonable and also necessary in today's operational environment.

The author believes that the Union’s efforts are a positive step forward, holding promising potential for success and certainly not doomed to failure. NIS2 has been designed to work alongside, and by supporting the standards and certifications that are already widely used. Problems will always arise with new legislation, and compromises have to be made, and flaws have to be fixed. Usually, some entity is on the losing side, financial or otherwise. The Directive is designed to strengthen the safety culture of all critical European organisations, not just those that are already well advanced.

7 Operational recommendations for media companies

The implementation date of the NIS2 is 17 October 2024. This means that companies should already at the time of writing this thesis understand what the legislation means for their activities. The authorities should be able assist in making decisions on the risk-management measures. The potential for significant compliance issues and damages connected to cybersecurity incidents is considerable, particularly now following the NIS2 Directive, which also introduces personal liability for management. It is therefore of paramount importance to comply with the relevant national legislation. Entities that are in the scope of the legislation, should start reviewing their cybersecurity measures for compliance issues, and get ready for the reporting obligations for if an incident occurs. This also means updating corporate policies and indicators for annual reporting. These actions will require an increase in the resources allocated to compliance and cybersecurity functions.

Given that public broadcasting companies are usually partly or wholly funded by taxpayers' money, this could potentially act as a multiplier when considering the extent of potential damages, particularly including reputational damage. This is because people may have certain expectations of public bodies that are not necessarily expected from others in the area of compliance. This is due to the fact that the general public is essentially the source of their funding. It might also be the case that a media company presents and upholds its position as an entity critical to society, similar to the way that Yleisradio does.[205] This may set expectations for this kind of a company to develop its operations on cybersecurity to a higher standard than smaller, less critical media companies.

All media organisations, regardless of size or scope, should be proactive in securing their systems. Media companies that have an important position in a member state, those that want to stay relevant in turbulent times, or those that want to defend their systems in the best possible way against cyberattacks, should consider reviewing their cybersecurity measures. The actual measures done by companies should not be motivated by legislation, but from the motivation for safeguarding their own business continuity from potential threats as part of basic risk management. It is not a

[205] Rajaniemi. ”Huoltovarmuus on uusi musta.” Article on the Perspective of Yleisradio on public broadcasting and security of supply.

requirement for every media company with these aspirations to implement the measures set out in the NIS2 in their activities. In preamble (13) NIS2, it is stated that “Given the intensification and increased sophistication of cyber threats, Member States should strive to ensure that entities that are excluded from the scope of this Directive achieve a high level of cybersecurity and to support the implementation of equivalent cybersecurity risk-management measures that reflect the sensitive nature of those entities.”

This is actually quite important to note. This means that even if an entity is not in the scope of application of the Directive, the cybersecurity risk-management measures of that entity should not be left under no scrutiny. If a media company is not under the scope of application of the NIS2 Directive, Member States should still make sure that the company achieves a high level of cybersecurity. Preambles are not binding legislation, but they provide valuable insight into the legislator's intent. Media companies, even if excluded from the Directive, should not overlook cybersecurity measures, as Member States are encouraged to promote equivalent measures. The cybersecurity measures taken by media companies not in the scope of the new directive-derived national legislation, should be made based on other applicable legislation and by recognised international and European standards. The objective of the Union legislator can be defined as the establishment of a European cybersecurity mindset based on a proactive and resilient security culture. This entails the integration of the safeguarding of systems against evolving threats as an inherent responsibility, transcending the mere regulatory obligation and shaping a new paradigm of security consciousness across all sectors, including the media.

Sauli Niinistö, the former President of the Republic of Finland and Special Adviser to the President of the European Commission recently prepared a report on Europe’s civil and military preparedness and readiness. The report emphasises the necessity for the EU to adapt to a rapidly evolving security environment, the Covid-19 pandemic, war and climate change. The EU should adopt an all-hazards, whole-of-government and whole-of-society approach, promoting public awareness, strengthening EU-NATO partnerships and allocating more resources to defence. The report highlights the significance of prompt decision-making, economic resilience and upholding a 'preparedness-by-design' mindset to effectively navigate future

crises and safeguard shared European principles and values.[206] This report is timely in providing guidance for the situation in Europe. Media companies could implement this "preparedness-by-design" principle in their business, the same way all organisations should, to uphold the objective explained by President Niinistö.

When determining the cybersecurity measures, an assessment has to be made internally. This assessment considers the criticality of the entity, the category of risks it is exposed to, the size of the entity, and the overall probability of an incident.[207] Also it could be argued that an entity should consider their risk appetite and tolerance when determining their cybersecurity measures.[208] This is in order to avoid disproportionate financial and administrative burden.[209] Media companies that are in the scope of the Directive are certainly in the scope not in the full extent of their activities. In situations like this, where some of entity's activities fall within the scope of the Directive, and some are excluded, guidance from the Commission is to be expected.[210] The adoption of cybersecurity measures by media companies is impacted by the fact that their core functions are not in the scope of the Directive. For media companies with both activities in and out of the scope, a tailored approach to cybersecurity is recommended. While awaiting more detailed guidance from the Commission, these companies should focus on securing their critical functions and strive to reach a reasonable level of cybersecurity across their entire operations. What follows is that the measures do not have to be, legally speaking and not considering sectoral legislation, as strict as an entity that is in the core definition of a category listed in the Annexes.[211] Ultimately, the level of adopted measures ultimately depend on the risk appetite and risk tolerance of the organisation in question.

---

[206] European Commission. "Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness." Executive Summary. 1–3.
[207] Preamble (82) NIS2.
[208] Risk appetite is the level of risk an entity is willing to take in their activities to reach their goals. This appetite and tolerance of risks needs to be carefully considered in any organisation.
[209] See preamble (81) NIS2.
[210] Preamble (21) NIS2 proposes that the Commission could provide guidance in situations like this.
[211] For example, Internet providers are in the core of the legislation and should closely look at the requirements of the Directive.

8 Conclusions and closing words

8.1 Conclusions

The NIS2 represents a revision of the rules governing the security of network and information systems of critical entities in the Union. It forms part of a wider programme of cybersecurity and conventional security development, and a shift of security mindset, driven by the Union, which has evolved since the proposal of the NIS2. The recent geopolitical events, including the US presidential elections and the uncertainties surrounding NATO, war in Ukraine and international relations have prompted the Union to seek an even better enhanced preparedness for the continuity of essential societal functions of the critical entities of the Member States. The NIS2 is timely in its entry into force in this respective.

NIS1 was too fragmented and did not work as effectively as the present situation needed it to. NIS2 was introduced, which promises to bring a more level playing field for critical entities. With this levelling act, comes new obligations for entities, both for those already in the scope of NIS1, but more importantly to those now to be included in the scope of the NIS2.

But the question of applicability of the Directive is not too simple for all organisations. One of those organisation types on the sidelines is the media. Media companies might not seem first as too critical for the functioning of society, at least to the level of infrastructure entities like those in energy and health or financial sectors. But imagine a situation where the society has been adversely impacted by something significant, and people want to be informed on actions one should take, for example if they need to stay inside or seek shelter. This is where media companies are in a key position. Media companies have the needed means and access to infrastructure that can reach people. This is why media companies are critical, even if not recognised by the Directive text.

Returning to the main research question of this thesis; *Do media companies fall under the scope of the NIS2 Directive?* Assessing whether media companies fall within the scope of the Directive is challenging. Nowhere in the Directive are media companies or even public broadcasters explicitly mentioned. The answer is not a definitive one that would cover all media companies or even all public broadcasting

companies. The final assessment must be made based on specific characteristics of individual companies by the member state implementing the Directive in coordination with the company itself, however the Member State decides to compile the list of critical entities in accordance with Article 27 of the NIS2, on basis of which the entities concerned have to register themselves to the competent authority.[212]

In particular, public broadcasting companies could very well be in the scope of the Directive, provided that they meet the criteria of the public administration sector, which are quite extensive. Meeting the criteria is not too simple, but the analysis shows that some companies can meet the criteria. For example, Yleisradio Oy has substantial justification for being included within the scope of application of the Directive and, as a consequence, within the national legislation implementing the Directive. This national legislation will take the individual characteristics of the Member State and the entity better into consideration. This does not mean that Member States where public broadcasting companies are not mandated the status of critical entities wouldn't have to consider the security of information distribution efforts during exceptional circumstances, or if under a severe cyberattack or hybrid operation. Conversely, it is imperative that all businesses implement robust cybersecurity measures. However, the level of these measures varies, and rightly so.

If a media company would own the network used, and thus could be defined as being included in the digital infrastructure sector of the Annex I of NIS2, the company would be in the scope of application the Directive. The deciding factor is the ownership of the network used. If the company uses a network provided by another entity, the cybersecurity requirements would in practice be included in the contract terms between those entities.[213] The same goes for any activity that a media company could have, that is included in the Annexes I and II of the NIS2. If an entity has any

---

[212] Article 27 NIS2 requires that entities submit the following information to competent authorities by 17 January 2025: (a) the name of the entity; (b) the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable; (c) the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3); (d) up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to Article 26(3); (e) the Member States where the entity provides services; and (f) the entity's IP ranges.
[213] The network provider would probably be included in the scope of application of the Directive, which would mean that the obligations of the Directive would apply the network provider directly, irrespective of what is agreed between contract parties. However, organisations in such a situation should require the other party to take effective risk management measures regardless of what the law provides.

activities in these sectors, it is in the scope of the Directive. If it does not, it is not in the scope of the Directive. To be included in this sector of digital infrastructure, the media company should own a public electronic communications network which is used “wholly or mainly for the provision of publicly available electronic communications services which support the transfer of information between network termination points.”

Media companies are by default excluded from the scope of the Directive. However, specific circumstances, such as ownership of the network used, the obligation to broadcast national emergency warnings, other national arrangements for the security of supply, and being defined as a public administration entity, decides if a media company is in the scope of application of the Directive.

Now to the supplementary research question; *What is the impact of the Directive on media companies operating within the Union?* The actual measures of the Directive are not in any way revolutionary. They are standard cybersecurity measures that critical companies should already have in place and are expected to by business partners or by already existing sectoral legislation. Bringing the bare minimum level of risk-management measures to the legislation is a positive development, as certainly not all entities in the scope have these, although very standard, measures in place. However, these new obligations could introduce difficulties for some entities, as they might require more work to achieve the same results, and this work is probably not tied directly to generating revenue.

The most substantial changes the Directive brings are the possibility for substantial fines, personal liability of management in entities not complying with the legal requirements for cybersecurity measures, and the requirement to give a 24-hour early warning to the CSIRTs or authorities. Guidelines for entities struggling are expected to come soon, which will help with the additional burden the legislation introduces. The possible introduction of more effective cybersecurity risk-management measures, those proposed by Ferguson, by supplementing acts would minimise the need for a complete revision of the Directive anytime soon.

8.2 Limitations of the study

This thesis was commissioned by Yleisradio Oy for internal and external use. Meetings have been held on informing the author of this thesis on the operations and structure of Yleisradio Oy. These meetings could have influenced my work, as the opinion of Yle's employees, and possible outcomes were discussed. Therefore, this thesis does have tendencies towards Yleisradio Oy and may lack in reaching the desired Europe-wide perspective. Complete objectivity could not be maintained, which is arguably often the case in scientific research. Conscious efforts have been made to reduce bias by using as wide a range of sources as reasonable, including non-Finnish sources and legislation, with attention to the wider legal landscape of the European Union.

Not much extensive research or literature has been written on this particular topic. This caused difficulties for the author of the study, as establishing a context for assessing the scope of NIS2 proved to be quite laborious. The study adds value particularly for the organisations assessing the scope of the new legislation and measures to be done in the wake of NIS2. Providing a definite answer that would concern all media companies in Europe is difficult, and most probably impossible. Other difficulties were mainly related to not focusing too much on the Finnish perspective on the organisation of society and Yleisradio Oy, to the assessment of the scope of the thesis, and to the author's time constraints.

This thesis was written from the perspective of a Finnish law student, which may influence my perception on the European Union's security landscape. This also means that the language used in this thesis is not at the level of a native speaker of the English language, and minor nuances may differ from those of a native speaker. Minor grammar errors might also occur.

Before I started working on this thesis, my knowledge of cybersecurity was very limited. This research and discussions with cybersecurity experts have greatly expanded my understanding of these areas. This knowledge has been applied to this thesis.

8.3 Closing words

Often it is said that regulation, in particular the European "genre" of regulation, hinders innovation and renders the operational environment for businesses difficult. This could also be a risk in cybersecurity regulation and the NIS2. The uncertainty of future regulation on cybersecurity causes difficulties for organisations and forces them to comply with existing legislation and at the same time prepare for upcoming legislation. On the other hand, if an organisation fails to adapt to new legislation, it subjects itself to legal and financial risks, but also to a non-competitive market position.[214] In today's business environment, cybersecurity has become a critical component of corporate compliance. The increasing scrutiny from regulators and the importance of credibility in eyes of customers are driving the need for adequate cybersecurity measures, now increasingly alongside mandatory legislation.

In the opinion of the author of this thesis, the Directive, along with other European cybersecurity, and conventional security developments, is a step to the right direction. New legislation always has its problems, particularly legislation concerning technology and obstacles like those with the NIS2 are inevitable. Ambiguities always exist, and it is specifically the legislators' and legal experts' job to shed light on regulation, and to help others in navigating the law. One could argue that rapid progress is needed, and that organisations just have to adapt to the new legislation. At the same time this kind of progress could have a negative effect on the short-term growth of the internal market. This is a risk that has to be taken if legislation is done sustainably.

For the European Union, it would be beneficial to provide guidance on how to navigate with the international standards, such as ISO 27001 and the Directive. The Commission is advised to provide guidelines on how to approach the question of the compatibility of the two. The standards are a very good starting point, but it would be beneficial for the entities, and for the European economy, to know if the standards, once inevitably updated to include the 24-hour early warning, are enough to prove compliance with the Directive. Right now, organisations are in a difficult position. Also, the actual risk-management measures, meaning incident prevention, should be

---

[214] Kianpour and Raza, "More than malware: unmasking the hidden risk of cybersecurity regulations." 203–204.

reviewed, as soon as possible and regularly, as they might just be of a lower standard than what is actually expected from organisations.

For entities assessing the scope of application of NIS2, it is important to remain cautious, but at the same time confident and strong. Influential and trusted media companies should have all of these very standard cybersecurity measures in place, regardless of the Directive and if its obligations concern them or not. What is important for entities, is to swiftly decide on their stance on the Directive, and to review their cybersecurity measures. This review and revision of cybersecurity measures should be carried out at least to the extent that the supervisor can be satisfied that some action has been taken, if that entity falls within the scope of national legislation.

Bibliography

Literature

Aarnio, Aulis. “Oikeussäännösten systematisointi ja tulkinta,” in Minun metodini, ed. Juha Häyhä, 35–56 , Werner Söderström lakitieto Oy, 1997.

Aarnio, Aulis. Essays on the Doctrinal Study of Law. 1st ed. Springer Dordrecht, 2011. https://doi.org/10.1007/978-94-007-1655-1.

Alén-Savikko, Anette. “Transparency in algorithmic journalism: from ethics to law and back” in Artificial Intelligence and the Media, Edward Elgar Publishing, 2022 accessed Aug 16, 2024. https://doi-org.libproxy.helsinki.fi/10.4337/9781839109973.00008.

Biasin, Elisabetta, and Kamenjašević, Erik. “Cybersecurity of medical devices: new challenges arising from the AI Act and NIS2 Directive proposals.” International Cybersecurity Law Review, Volume 3, 163–180, Springer Nature, 2022. https://doi.org/10.1365/s43439-022-00054-x.

Boggini, Clara. “Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework.” Computer Law & Security Review, Volume 53, 2024. https://doi.org/10.1016/j.clsr.2024.105987.

Calder, Alan. Network and Information Systems (NIS) Regulations - a Pocket Guide for Operators of Essential Services. IT Governance Ltd, 2018.

Caranta, Roberto, Edelstam, Gunilla and Trybus, Martin. EU Public Contract Law: Public Procurement and Beyond. Bruylant, Editions juridiques, 2013.

Cerulus, Laurens, “EU Sanctions Russian Hackers for 2015 Bundestag Breach,” POLITICO, 22 October 2020. Accessed 7 February 2024. https://www.politico.eu/article/eu-sanctions-russias-fancy-bear-hackers-for-2015-bundestag-breach/.

Eckhardt, Philipp. “NIS2 Directive: New EU Rules on Cybersecurity.” cepAdhoc, no.9/2022. Centrum für Europäische Politik, 2022. https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepAdhoc_NIS_2.0/cepAdhoc_NIS_2_Directive_New_EU_Rules_on_Cybersecurity.pdf.

Eskola, Saila, Kiviniemi, Eeva, Krakau, Tarja, and Ruohoniemi, Erkko. Julkiset Hankinnat. 3. uudistettu painos. Alma Talent 2017.

Ferguson, D.D.S. “The outcome efficacy of the entity risk management requirements of the NIS2 Directive.” International Cybersecurity Law Review. Volume 4, 371–386. Springer Nature, 2023.

Filiol, Eric, Mercaldo, Francesco, and Santone, Antonella. “A Method for Automatic Penetration Testing and Mitigation: A Red Hat Approach.” Procedia Computer Science, Volume 192, Elsevier B. V., 2021. https://doi.org/10.1016/j.procs.2021.08.210.

Hirvonen, Ari. Mitkä metodit? : Opas oikeustieteen metodologiaan. Helsingin yliopisto, Oikeustieteellinen tiedekunta, 2011. https://helda.helsinki.fi/items/9f946224-556d-4b2e-a071-d23a6cfa78b6.

Hoecke, Mark Van. "Legal Doctrine: Which Method(s) for What Kind of Discipline?." In Methodologies of Legal Research: What Kind of Method for What Kind of Discipline?, ed. Mark Van Hoecke, 1–18. Hart Publishing, 2011. http://dx.doi.org/10.5040/9781472560896.ch-001.

Kangas, Urpo. “Minun metodini”, in Minun metodini, ed. Juha Häyhä, 90–109, Werner Söderström lakitieto Oy, 1997.

Keinänen, Anssi, and Väätänen, Ulla: ”Empiirinen oikeustutkimus – mitä ja milloin?,” in Oikeustieteellinen opinnäyte – artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta, ed. Tarmo Miettinen. Edita Publishing Oy, 2016.

Kianpour, Mazaher, and Raza, Shahid. “More than malware: unmasking the hidden risk of cybersecurity regulations.” International Cybersecurity Law Review, Volume 5, 169–212. Springer Nature, 2024.

Lenaerts, Koen, and Gutiérrez-Fons, José A. “To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice.” Distinguished Lectures of the Academy, Working paper, European University Institute, Academy of European Law, 2013.

Lianos, Ioannis, and Odudu, Okeoghene. Regulating Trade in Services in the EU and the WTO : Trust, Distrust and Economic Integration. Cambridge University Press, 2012.

Mäntysaari, Petri. ”Onko legal design tiede? Havaintoja erään väitöskirjan perusteella.” Lakimies, 1/2024: 174–188. https://journal.fi/lakimies/article/view/138010.

Murr, Mike. “SEC504.I Incident Response and Computer Crime Investigations.” In SEC504: Hacker Tools, Techniques, and Incident Handling, SANS Institute, 2020.

Ojanen, Tuomas. EU-Oikeuden Perusteita. 3., Uudistettu laitos. Edita Publishing Oy, 2016.

Parcu, Pier Luigi, and Brogi, Elda. “Introduction to Research Handbook on EU Media Law and Policy: understanding the EU approach to media law and policy. The scope of the Handbook and a presentation of the contributions.” In Research Handbook on EU Media Law and Policy. Edward Elgar Publishing, 2021. https://doi-org.libproxy.helsinki.fi/10.4337/9781786439338.00005.

Rautiainen, Pauli, Kostiainen, Aura, Kurki, Visa, Soininen, Niko, and Määttä, Tapio. Oikeus ja sen tutkiminen. Vastapaino, 2023.

Sajama, Seppo. ”Argumentaatio Oikeustieteellisessä Tutkimuksessa.” In Oikeustieteellinen Opinnäyte – Artikkeleita Oikeustieteellisten Opinnäytteiden Vaatimuksista, Metodista Ja Arvostelusta, edited by Tarmo Miettinen. Edita Publishing Oy, 2016.

Sajama, Seppo. ”Mikä tekee tutkimuksesta tieteellisen?” in Oikeustieteellinen opinnäyte – artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta, edited by Tarmo Miettinen, Edita Publishing Oy, 2016.

Savigny, Friedrich Carl von. System des heutigen Römischen Rechts. Volume 1. Deutsches Textarchiv, Berlin, 1840, accessed 4 March 2024. https://www.deutschestextarchiv.de/savigny_system01_1840.

Schmitz-Berndt, Sandra, and Chiara, Pier Giorgio. “One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive.” International Cybersecurity Law Review, volume 3, 289–311. Springer Nature, 2022. https://doi.org/10.1365/s43439-022-00058-7.

Schmitz-Berndt, Sandra. “Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS2 Directive.” Journal of Cybersecurity, 1–11. Oxford University Press, 2023. https://doi.org/10.1093/cybsec/tyad009.

Siemers, David J., The Myth of Coequal Branches: Restoring the Constitution’s Separation of Functions. University of Missouri, 2018. https://search-ebscohost-

com.libproxy.helsinki.fi/login.aspx?direct=true&db=e000xww&AN=1921073&site=ehost-live&scope=site.

Sievers, Thomas. “Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations.” International Cybersecurity Law Review, Volume 2, Springer Nature, 2021. https://doi-org.libproxy.helsinki.fi/10.1365/s43439-021-00033-8.

Sutton, David. Cyber Security: The Complete Guide to Cyber Threats and Protection. 2nd edition. BCS Learning & Development Limited, 2022. ProQuest Ebook Central. https://ebookcentral-proquest-com.libproxy.helsinki.fi/lib/helsinki-ebooks/detail.action?docID=7146447.

Van Gestel, Rob, and Micklitz, Hans-W. Revitalizing Doctrinal Legal Research in Europe: What About Methodology? Working paper no. 2011/05, European University Institute, Department of Law, 2011. https://ssrn.com/abstract=1824237.

Vandezande, Niels. “Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor.” Computer Law & Security Review, volume 52 (2024). https://doi.org/10.1016/j.clsr.2023.105890.

Vile, M. J. C.. Constitutionalism and the Separation of Powers, 2nd edition, Liberty Fund, Incorporated, 1998. ProQuest Ebook Central. https://ebookcentral-proquest-com.libproxy.helsinki.fi/lib/helsinki-ebooks/detail.action?docID=3327330.

Official sources

Directorate-General for Parliamentary Research Services Bassot, Étienne, European Parliament, ‘Ten issues to watch in 2023 – In-depth analysis.” January 2023. https://data.europa.eu/doi/10.2861/594.

European Commission. “Communication from the Commission on the application of State aid rules to public service broadcasting.” OJ C 257.

European Commission. “Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.” Explanatory memorandum, COM(2020) 823 final.

European Commission. “Report from the Commission to the European Parliament and the Council: assessing the consistency of the approaches taken by Member

States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems." COM(2019) 546 final.

European Commission. "Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness. Report by Special Adviser Niinistö." https://commission.europa.eu/topics/defence/safer-together-path-towards-fully-prepared-union_en.

European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Shaping Europe's digital future." COM(2020) 67 final.

European Commission. Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy." JOIN/2023/20 final.

European Commission. Joint Communication to the European Parliament and the Council: "The EU's Cybersecurity Strategy for the Digital Decade." JOIN/2020/18 final.

European Council, General Secretariat of the Council. "Special Meeting of the European Council, 17 and 18 April 2024 – Conclusions." EUCO 12/24,

He 57/2024 vp.

Valtioneuvoston päätös huoltovarmuuden tavoitteista 1048/2018.

Legislation

BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 29. November 2023 (BGBl. 2023 I Nr. 339) geändert worden ist.

Commission Directive 2006/111/EC of 16 November 2006 on the transparency of financial relations between Member States and public undertakings as well as on financial transparency within certain undertakings, OJ L 318/17.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194.

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of

certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, OJ L303/69.

Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting, OJ L 322/15.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive), OJ L 333/80.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). L 201/37.

Directive 2014/23/EU of the European Parliament and of the Council of 26 February 2014 on the award of concession contracts, OJ L 94/1.

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, OJ L 94/65.

Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC, OJ L 94/243.

Hallintolaki 434/2003.

Laki julkisista hankinnoista 1397/2016.

Laki sähköisen viestinnän palveluista, 917/2014.

Laki Vaaratiedotteesta, 466/2012.

Laki Yleisradiosta 1380/1993. English translation available here: https://www.finlex.fi/fi/laki/kaannokset/1993/en19931380_20170436.pdf.

Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, 2024202344.

Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation), OJ L 119.

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151.

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333/1.

Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act) OJ L series.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L series.

Zakon o Hrvatskoj radioteleviziji, NN 137/2010-3515.

Zakon o kibernetičkoj sigurnosti, NN 14/2024-254.

Case Law

Case 283/81 CILFIT.

Case C-31/87 Beentjes v. Netherlands.

Case C-337/05 Commission v. Italy (Agusta and Agusta Bell Helicopters).
Joined Cases C-21/03 and C-34/03 Fabricom SA v Belgium.

Other sources

Arcidiacono, Antonio. “Can We Keep the Information Flowing?” EBU, Technology & Innovation, 28 November 2023. Accessed 21 February 2024. https://tech.ebu.ch/news/2023/11/can-we-keep-the-information-flowing.

Berkeley, University of California. “Frequently Asked Questions – Ransomware”, Information Security Office. Accessed 7 February 2024. https://security.berkeley.edu/faq/ransomware/.

Cambridge University Press & Assessment, Cambridge Dictionary. “most.” Accessed 3 October 2024. https://dictionary.cambridge.org/us/dictionary/english/most.

Cambridge University Press & Assessment, Cambridge Dictionary. “the Fourth Estate.” Accessed 3 October 2024. https://dictionary.cambridge.org/dictionary/english/fourth-estate.

Crossroads Bank for Enterprises, “Public Search Tool.” Accessed September 16, 2024. https://kbopub.economie.fgov.be/kbopub/zoeknummerform.html.

Der Spiegel. ”Russische Gruppe »Ghostwriter« attackiert offenbar Parlamentarier.” March 26, 2021. Accessed 7 February 2024. https://www.spiegel.de/politik/deutschland/russischer-hack-erneute-attacke-hack-auf-bundestag-sieben-abgeordnete-betroffen-a-75e1adbe-4462-4e30-bd94-96796aed6b8a.

EBU. “About the EBU.” Accessed 4 October 2024. https://www.ebu.ch/about.

Eduskunta. ”Eduskuntaan on kohdistunut kyberhyökkäys.” Accessed 7 February 2024. https://www.eduskunta.fi:443/FI/tiedotteet/Sivut/Eduskuntaan-on-kohdistunut-kyberhy%C3%B6kk%C3%A4ys.aspx.

European Broadcasting Union (EBU). “Our Members.” Accessed 1 October 2024. https://www.ebu.ch/about/members.

European Commission. “Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – FAQs.” Accessed 25 September. https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs.

European Commission. “Public Procurement.” Accessed 19 May 2024. https://defence-industry-space.ec.europa.eu/funding-opportunities-0/public-procurement_en.

European Commission. Infographic, “Main actors and Networks of cooperation involved in the Joint Cyber Unit.” June 2021. Available at https://digital-strategy.ec.europa.eu/en/library/infographic-eu-cybersecurity-ecosystem.

Eurostat. "Enterprises experienced ICT related security incidents leading to consequences, EU, 2021." ICT Security in Enterprises. Accessed 15 September 2024. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises.

Harper, Rebecca. “NIS2: What The Proposed Changes Mean For Your Business.” ISMS, 9 April 2023. Accessed 25 September 2024. https://www.isms.online/cyber-security/nis-2-what-the-proposed-changes-mean-for-your-business/.

HRT, “Javna nabava.” Accessed 16 September 2024. https://o-nama.hrt.hr/nabava/javna-nabava-4848.

HRT, “O HRT-u.” Accessed 16 September 2024. https://o-nama.hrt.hr/hrt/o-hrt-u-774.

Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats). “Countering Disinformation: News Media and Legal Resilience.” Workshop paper 1, November 2019. https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf

International Telecommunication Union ITU, “Radio Regulations,” Edition of 2020. Available at https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/1.44.48.en.101.pdf.

Kahmen, Jan. “The Relationship Between NIS2 and ISO 27001.“ Turingpoint GmbH, 9 June 2024. Accessed 1 October 2024. https://turingpoint.de/en/blog/the-relationship-between-nis-2-and-iso-27001/.

Morgan, Steve. “2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics.” Cybercrime Magazine, 19 January 2022. https://cybersecurityventures.com/cybersecurity-almanac-2022/.

Morgan, Steve. “Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031.” Cybercrime Magazine, 1 June 2021. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

OECD. “Public Procurement – OECD.” Accessed 19 May 2024, https://www.oecd.org/governance/public-procurement/.

Plasman, Dries. “Is ISO 27001 enough for NIS2 compliance?” Ceeyu BV, 21 February 2024. Accessed 1 October 2024. https://www.ceeyu.io/resources/blog/is-iso-27001-enough-for-nis-2-compliance.

Rajaniemi, Petri. ”Huoltovarmuus on uusi musta.” Yleisradio, 9 September 2024. Accessed 1 October 2024. https://yle.fi/aihe/a/20-10006982.

Sonia Lilja. “CER- ja NIS2-direktiiviehdotusten vaikutus mediayhtiön varautumiseen: Case Yleisradio Oy.” Thesis, Laurea-ammattikorkeakoulu, 2023. Available here: https://www.theseus.fi/bitstream/handle/10024/789364/Lilja_Sonia.pdf?sequence=2.

SVT. “SVT och pengarna - Året med SVT.” Accessed 21 February 2024. https://aretmedsvt.svt.se/svt-och-pengarna.

SVT. ”Jobba här.” Accessed 14 March 2024. https://omoss.svt.se/jobba-har.html.

UR. “Om public service.” Accessed 21 March 2024. https://www.ur.se/om-oss/om-public-service/.

Valtioneuvosto, Statsrådet [@valtioneuvosto]. ”Valtioneuvoston ja ministeriöiden verkkosivustoihin kohdistuu tällä hetkellä palvelunestohyökkäys. Osa ministeriöiden sivustoista ei toimi lainkaan tai osin. http://Valtioneuvosto.fi, joka kokoaa ministeriöiden tiedotteet, toimii tällä hetkellä normaalisti.” Twitter (now X), 8 April 2022. https://twitter.com/valtioneuvosto/status/1512371948889722887.

Yleisradio Oy. “Hankinnat – näin Yle hankkii tavaroita ja palveluja.” Accessed 25 May 2024. https://yle.fi/aihe/s/ylen-hankinnat.

Yleisradio Oy. “Yle’s Annual report 2023.” https://yle.fi/aihe/yles-year-2023.

Yleisradio Oy. “Ylen talous.” accessed 25 May 2024. https://yle.fi/aihe/yleisradio/talous.

Yleisradio Oy. ”Henkilöstön avainluvut 2022.” Accessed 21 February 2024. https://yle.fi/aihe/s/10004491.