UNIVERSITY OF HELSINKI

Faculty of Law

Proposing new EU legislation to bridge the existing gap between current European cybersecurity legislation and enterprise cybersecurity

Thesis
Faculty of Law
Viivi Nuorti
5.9.2021

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Abstract

Faculty: Faculty of Law

Degree programme: International Business Law

Author: Viivi Nuorti

Title: Proposing new EU legislation to bridge the existing gap between current European cybersecurity legislation and enterprise cybersecurity

Level: Master's Thesis

Month and Year: September 2021

Number of pages: 72

Keywords: cybersecurity legislation, operational technologies, enterprise technologies, digital infrastructure

Supervisor: Ville Pönkä

Abstract:

This thesis proposes new EU legislation to bridge the gap between current European cybersecurity regulation and enterprise operational technologies. Considering the fast development and expansion of technologies within our society, our legal thinking and the adoption of protective measures in the form of new EU legislation is paramount, if not critical, in order to sufficiently protect the operations and undisrupted contingency of critical infrastructure's enterprises, our digital service providers, and the services provided by our essential operators.

The EU Cybersecurity Act, Network and Information Security Directive, the proposed revised NIS2 Directive, and the European Union Agency for Cybersecurity (ENISA) are the foundation of tomorrow's digitized and secure Europe. However, they exclude the technologies closest to the core manufacturing and service-production of an enterprise: the operational technologies solutions.

The main questions of this thesis were whether a sufficient layer of mandated cybersecurity protection for connected enterprises and digital infrastructure exists, how small operational technologies solution vendors and digital service providers could be required to take responsibility for the cybersecurity of their solutions, and why does the proposed legally required framework for operational technologies matter.

The legal and technical analysis concludes that the principle of security by design is not widely adopted within modern digitized enterprises, which sets a poor basis for the Single Digital Market. Currently, the burden of executing a well-managed enterprise security office lies on the shoulders of the enterprise's CIO and CISO officers.

IT leaders lack a steering certification framework that sufficiently covers the complete IT environment with security principles and actionable requirements.

This thesis proposes that operational technologies are included in the next scope of the next revision of EU cybersecurity legislation. The elements of the proposed framework would help in protecting European connected enterprises, and to support EU in achieving high-level cybersecurity cooperation and protection within the European Digital Market. This thesis could be utilized in the drafting of the candidate cybersecurity certification scheme EUCC.

The aimed readership includes EU's legislators, and executives that work with enterprise technologies, digital infrastructure, and cloud-native technologies.

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiivistelmä

Yksikkö: Oikeustieteellinen tiedekunta

Pääaine: Kansainvälinen yritysjuridiikka

Tekijä: Viivi Nuorti

Työn nimi: Uuden EU-lainsäädännön ehdottaminen nykyisen EU kyberturvallisuuslainsäädännön ja yritysten turvallisuuden välisen kuilun umpeen kuromiseksi

Työn laji: Pro-gradu -tutkielma

Kuukausi ja vuosi: Syyskuu 2021

Sivumäärä: 72

Avainsanat: kyberturvallisuus, lainsäädäntö, operatiiviset teknologiat, digitaalinen infrastruktuuri, konserniteknologiat

Ohjaaja: Ville Pönkä

Tiivistelmä:

Teknologian avulla voimme muun muassa kommunikoida, tallettaa tietoa ja ratkaista ongelmia fiksummin kuin koskaan. Kuitenkin kääntöpuolena uuden teknologian mukana tulee uusia riskejä, joita pitää hallinnoida. Tämä on haaste, jonka yhtiöiden johtoryhmät, valtionhallinnot ja tietenkin kaikkein korkeimmalla hallinnon tasolla, Euroopan Unioni kohtaavat. Kyberturvallisuus on elintärkeää yhtiöiden ja valtioiden vakauden ja jatkuvuuden kannalta – eurooppalainen digitaalinen ja kriittinen infrastruktuuri ovat enenemissä määrin haitallisten hyökkäysten kohteena, ja siksi on tärkeää sisällyttää turvallisuus tärkeimmäksi lainsäädännön muotoilua ohjaavaksi periaatteeksi EU:n kyberturvallisuuslainsäädäntöön.

Tämä pro gradu -tutkielma ehdottaa uutta EU-lainsäädäntöä nykyisen kyberturvallisuuslainsäädännön ja yritysten operatiivisten teknologioiden kyberturvallisuuden välisen kuilun umpeen kuromiseksi. Nykyinen EU:n kyberturvallisuusasetus, kyberturvallisuusdirektiivi (NIS), ehdotettu uudistettu kyberturvallisuusdirektiivi (NIS2) sekä Euroopan unionin verkko- ja tietoturvaviraston (ENISA) julkaisemat viralliset ohjeet luovat perustaa tulevaisuuden digitaaliselle Euroopalle. Olemassa oleva EU-lainsäädäntö sääntelee infrastruktuurin ja verkkotasolla turvallisuusstrategioista, arkkitehtuurista, valvonnasta ja säädäntövallasta. Kuitenkin sääntelyn ulkopuolelle jää huomattava osa siitä teknologiasta, jonka varassa yhtiöt ja virastot toimivat: operatiiviset teknologiat. Nykyisen lainsäädännön puute on, että se ei velvoita yhtiöitä ja virastoja pitämään yllä turvallisuusprosesseja ja -dokumentaatiota kaikkien sen käyttämien ohjelmistojen osalta.

Tällä hetkellä vastuu hyvin toteutetusta yhtiön digiturvallisuudesta jää yksittäisten tietohallintojohtajien (CIO) ja

tietoturvajohtajien (CISO) harteille. Näiden henkilöiden toiminnan taustalta on jo pitkään puuttunut EU lainsäädännön ohjaava toiminta. Turvallisuuden periaatteita ei olla rakennettu osaksi nykyisiä digitaalisia yhtiöitä ja virastoja, joissa kuitenkin käytetään jatkuvasti kehittyviä uusia operatiivisia teknologioita ja monimutkaisia toisiinsa liitettyjä verkkoavaruuksia.

Tämä pro gradu -tutkielma selittää, miksi nykyinen EU-lainsäädäntö ja ENISA yhdessä eivät riittävästi suojaa Euroopan digitaalista infrastruktuuria, sekä yhtiöitä ja virastoja. Lisäksi tutkielmassa ehdotetaan uutta viitekehystä, jolla olemassa olevaa lainsääntöä voitaisiin ohjata operatiivisten teknologioiden turvaamiseksi jatkossa. Tutkielman tarkoitus on siis ehdottaa EU komissiolle, että operatiiviset teknologiat tulisi sisällyttää pakollisen sääntelyn piiriin, jolla suojellaan eurooppalaisia toisiinsa kytkeytyneitä yhtiöitä. Lisäksi tarkoituksena on tukea EU:ta siinä, että unionissa saavutettaisi yhtenäinen ja korkea kyberturvallisuuden taso.

Työryhmän ensiversiona julkaistu tulevaisuuden kyberturvallisuuden sertifikaattikehys EUCC olisi potentiaalinen julkaisu, jossa tämän tutkielman esittämää viitekehystä voisi hyödyntää.

Tämä pro gradu -tutkielma on tarkoitettu erityisesti EU lainsäätäjille, IT-, liiketoiminnan-, ja lainsäädännön ammattilaisille sekä johtohenkilöille, jotka tekevät töitä konserniteknologioiden ja digitaalisen infrastruktuurin tai pilvinatiivien teknologioiden parissa.

Contents

ABBREVIATIONS

CaaS
Cyber(security) as a Service

ENISA
European Union Agency for Network and Information Security IaaS
Infrastructure as a Service

IAM
Identity and access management. Enterprises monitor and limit access to different parts of an enterprise's networks, databases, and solutions based on role (i.e. administrator), divisional and professional need based of access among other reasons.

Next-generation environments
Describes highly automated and connected networks and environments

OT
Operational Technologies

OT SEC
Operational technologies security

PaaS
Platform as a Service

SaaS
Software as a Service

Technology stack
A technology stack, also called a solutions stack, technology infrastructure, or a data ecosystem, is a list of all the technology services used to build and run one single application.

OES

Operator of Essential Service, often considered to be a part of the critical infrastructure European Union Member States rely upon

DSP

Digital Service Provider; search engine, online marketplace, cloud computing service providers

REFERENCES

Literature

Aarnio, A. 1997. *Oikeussäännön systematisointi ja tulkinta*. WSOY, Helsinki.

Anton S., Fraunholz D., Krohmer D., Reti D., Schneider D., Schotten H. D. 2021. The Global State of Security in Industrial Control Systems: An Empirical Analysis of Vulnerabilities around the World. *IEEE internet of things journal*. p.1-5

Benincasa, E. 2021. The Case for Cyber 'Disarmament' in the European Union. 2021. *The International spectator* 56 (1), p.39-54

Cadler, Alan. 2018. Network and Information Systems (NIS) Regulations: a pocket guide for digital service providers. *IT Governance*

Caldwell, Tracey. 2018. Plugging IT/OT Vulnerabilities. *Network Security* Volume 09 (9) p. 10-15

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby H & Stoddart, K. 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security* 56, p-1-27

Christou, G. 2018. The challenges of cybercrime governance in the European Union. *European politics and society* 19 (3), p.355-375

Conklin, A. 2016. IT vs OT Security: A Time to Consider a Change in CIA to Include Resilience. 49th Hawaii International Conference on System Sciences, *IEEE Computer Society* Volume 49. p. 2642

Galinec, D., Možnik, D. & Guberina, B. 2017. Cybersecurity and cyber defence: national level strategic approach. *Automatika* 58(3), p 273-286

Gestel, R., Micklitz, H. & Rubin, E. 2017. Rethinking Legal Scholarship: A Transatlantic Dialogue. *Cambridge University Press*

Gomez, Camilo. 2019. Proactive management of plant cybersecurity. *Control Engineering*. Volume 66 (2) p. 20 – 22

Gosine, Anil. January 2017. Incorporating cybersecurity awareness into OT. *Control Engineering Journal* Volume 64 (1) p.DE1-DE2

Hale, Greg. 2020. IIoT's growing impact on ICS cybersecurity. *Control Engineering*. Volume 67 (11). p. 46

Hemsley, K., & Fisher, R. 2018. History of Industrial Control System Cyber Incidents. United States. https://doi.org/10.2172/1505628. Referenced 21.4.2021

Hirvonen, A. 2011. Mitkä metodit? Opas oikeustieteen metodologiaan. *Yleisen oikeustieteen julkaisuja* 17. Helsinki

Iaiani, M., Tugnoli, A., Bonvicini, S. & Cozzani, V. 2021. Major accidents triggered by malicious manipulations of the control system in process facilities. *Safety Science* 134, article 105043

Kontargyris, X. 2018. IT Laws in the Era of Cloud Computing: A Comparative Analysis between EU and US Law on the Case Study of Data Protection and Privacy

Markopoulou, D. & Papakonstantinoua, V. & Hert, P. 2019. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review* 35 (6)

Marston, S., Li, Z., Bandyopadhyay, S., Zhanga, J. & Ghalsasi, A. 2011. Cloud computing – The business perspective. *Decision Support Systems* 51 (1), p. 176-189

Moreno, C., V., Reniers, G., Salzano, E. & Cozzani, V. 2018. Analysis of physical and cyber security-related events in the chemical and process industry. *Process Safety and Environmental Protection* 116, p. 621-631

Narendra, M. & Singh, R.K. 2020. Prioritization and Security Defense Algorithm for Cloud Specific Vulnerability Through Scoring and Base Metric Group. *Journal of Interdisciplinary Mathematics.* Volume 23 (2), p. 481-491

Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H., 2012. SCADA security in the light of cyber-warfare. *Computers & Security* 31 (4) p. 418-436

Nomos Verlagsgesellschaft mbH & Co. KG. ISBN: 3845295627

OECD (Organisation for Economic Co-operation and Development). 2015. Towards a Framework for the Governance of Infrastructure. Paris: OECD. Available at https://www.oecd.org/gov/budgeting/Towards-a-Framework-for-the-Governance-of-Infrastructure.pdf. Referenced 18.8.2021

Solor, Amir. 2020. Six ways to improve cybersecurity: Barriers vs. resiliency. *Control Engineering* Volume 67 (11) p. 35-36

Tuunanen, T., Kazan, E., Salo, M., Leskelä, R., & Gupta, S. 2019. From digitalization to cybernization: Delivering value with cybernized services. Scandinavian *Journal of Information Systems 31* (2), Article 3

Wright D., de Hert P. Enforcing privacy. 2016. *The Law-Governance and Technology Series*. (25), p.227

Other references

EUISS, European Commission External Action, European Commission. Internationalizing critical infrastructure and functions protection. 2020. *Online webinar*. Sourced 19.8.2021

ENISA Strategy - A Trusted and Cyber Secure Europe (in 23 EU languages). 17.7.2020. Available at https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy/view. Referenced 20.4.2021

ENISA. Cybersecurity certification, EUCC, a candidate cybersecurity sertification scheme to serve as a successor to the existing SOG-IS. Available at file:///C:/Users/mvaananen/Downloads/ENISA_Candidate_Scheme_EUCC_v1.1.1.pdf. 1.9.2021

European Central Bank. G7 fundamental elements of cybersecurity for the financial sector. 2016. Available at G7_Fundamental_Elements_Oct_2016.pdf (europa.eu). Referenced 1.9.2021

European Commission. Cybersecurity policies. Available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#ecl-inpage-kmq7iavv. Referenced 28.8.2021

European Commission 2020a. Study on critical dependencies of energy, finance and transport infrastructures on ICT infrastructures. 8.3.2020. Referenced 1.5.2021

Europe's Digital Decade: Digital targets for 2030. Available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en. Referenced 23.8.2021

European Commission 2020b. Counter terrorism and radicalisation: Protection. Available at https://ec.europa.eu/home-affairs/what-we-do/policies/counter- terrorism/protection_en. Referenced 3.4.2021

European Commission 2020c. A Europe fit for the digital age. Available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age. Referenced 9.8.2021

European Commission 2020d. The European Digital Strategy. Available at https://ec.europa.eu/digital- single-market/en/content/european-digital-strategy 28.8.2021

European Commission 2016. Directive on Security of Network and Information Systems (NIS) *Official Journal of the European Commission*. 6.7.2016. Available at https://eur-lex.europa.eu/eli/dir/2016/1148/oj. Referenced 11.3.2021

European Commission 2021a. Revised Directive on Security of Network and Information Systems (NIS2) Fact Sheet. https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2. Referenced 8.5.2021

European Commission 2021b. The EU Cybersecurity Act Q&A. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369. Referenced 29.3.2021

COM/2009/0149 final. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection*. Available at https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52009DC0149. Sourced 2.3.2021

KPMG Harvey Nash 2019 CIO Survey. 2019. https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/07/harvey-nash-kpmg-cio-survey-2019.PDF. Referenced 13.3.2021

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience. https://www.cisa.gov/critical-infrastructure-sectors. Referenced 1.3.2021

Legislation

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*. (europa.eu)

Cybersecurity Act 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. (europa.eu)

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (europa.eu)

Directive 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. EUR-Lex - 32016L1148 - EN - EUR-Lex (europa.eu)

Directive (Eu) 2019/1937 Of The European Parliament And Of The Council of 23 October 2019 on the protection of persons who report breaches of Union law Directive (eu) 2019/1937 of the European Parliament

The Common Foreign and Security Policy (CFSP) of the European Union. 2009. European Union

Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity

Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security

Regulation No 549/2004/EC of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky

Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area

Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions

Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare

Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption

FIGURES

Tables

1 Introduction

1.1 Background

Considering the fast development and expansion of technologies and their ever-deepening adoption within our society, our legal thinking and legislative adoption of new protective measures in the form of EU Regulations is paramount, if not critical, to sufficiently protect the operations and undisrupted contingency of enterprises, especially those that are a part of our critical infrastructure. Enterprises with their operations, services, and digital infrastructure have become increasingly important to economic and human wellbeing in Europe. Possible disruptions can have catastrophic consequences, with negative spillover affecting not only business continuity of other critical infrastructure entities, but a much wider audience of European economic, infrastructure, and, and human members.

Digital infrastructure's enterprises and actors of the connected enterprises should be mandated to create and maintain security strategies and plans of action with a framework that can be tailored to their complexity, risk profile, and significance. Such framework should be structured in a unified way, so that it could be effectively audited by appointed government officials.

This thesis introduces a tool for creating sufficient and safe digital infrastructure, and monitoring enterprise-level and network-level security strategies and digital infrastructure in European modern enterprises. The current legislative frameworks and the role of ENISA leaves a significant gap between mandated requirements and what are often called as industry best practices or ENISA's recommendations. Therefore, the minimum requirements in current, mostly non-existing cybersecurity requirements, are far from the reality of what is actually needed to sufficiently protect continuously developing digital infrastructure, as in figure 1. Legislation is slow to adapt to technical developments and innovations, which can be seen I the way the current European cybersecurity legislation NIS has been created; whenever legislation is drafted and revised to take in consideration and within its' scope to permit new innovations, the designing and releasing of new novel technologies has already happened a multitude of occasions. Therefore the way new EU legislation is drafted should be done in a matter where both introducing defensive mechanism meant to limit adoption of novel technologies and those that allow for increased adoption of solutions are both agile and quick to implement. This thesis

introduces a framework that can bridge the current gap between ENISA's industry standard best practices and mandated protective measures in European Union's legislation. With the introduced framework, adaptation of protective measures and ensuring sufficient monitoring is in place is no longer an option for companies. Such framework indirectly would impact both European economic and human safety, as our digital infrastructure and networks are less vulnerable to hostile attacks, safety increases. Europe needs its own updated certification framework for cybersecurity requirements with flexibility and scalability to fit all circumstances and target organizations.

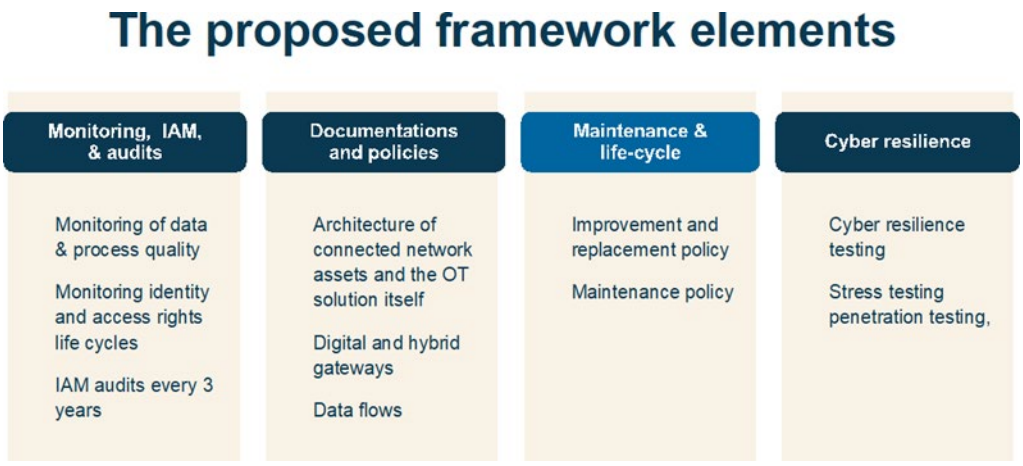

Figure 1: Overview of the proposed framework elements that help include operational technologies security in the European Union's Cybersecurity Act. The framework includes both physical and digital elements.

Ten years back in my career, I was heavily focused on operational technologies software and solution development as a Chief Technology Officer and headed a company that developed solutions for resources industries clients. I gained hands-on experience working with some of the largest manufacturers and energy producers in Europe, developing specific-purpose automation and operational technologies solutions that automate processes on the factory floors, closest to the core business of the enterprise. The deeper I dove into enterprise architecture and the connected nature of them, the more concerned I grew. Vulnerabilities were easy to spot, processes and architecture were not documented, maintenance, patching and lifecycle management only existed in the unspoken plans of the leaders of the IT department of the enterprise. Too often real, clear, and concise plans did not exist outside the everyday

operations that directly impacted service continuity and reliability. While I was working with operational technologies, Throughout the time I worked with developing operational technologies solutions, I studied cybersecurity legislation in the United States, and at later time in Europe.

I currently design, plan, and lead large digital transformation programs of Fortune 500 enterprises across Europe for various industries. In the last ten years, I have not seen much progress in terms of the adoption of voluntary cybersecurity design principles in European enterprises, and as a personal estimate, we are years behind the United States market in unified certifications that are fit to our market, European cybersecurity legislation, and punitive measures. During the last decade, at best, Europe has relied heavily on the lead of the United States on all cybersecurity related actions, instead of focusing on the legacy. Our markets, though there are many similarities, cannot be compared at face value. In 2019, the strengthening cooperation between Member States and mandates awarded to ENISA are a step to the right direction in redesigning the design elements of European Digital Infrastructure. The pillars that we currently have built our digital infrastructure upon are reliability and operational safety. Security, the most important pillar to hold the foundation of our digital infrastructure still needs to be built with the help of legislative action and the strengthened ENISA. Over a decade of hands on work designing secure enterprise IT environments, and work in developing novel operational technologies solutions, combined with legal education and interest in European cybersecurity legislation incited me to propose the framework that is introduced in this thesis.

1.2 Research questions

The objective of this thesis is to propose a new framework requirement to be added to the current European cyber regulation and official security guidelines from both a legal and technical perspective, in order to analyze the existing gap on the recommended and mandatory cybersecurity measures the critical infrastructure's enterprises and networks currently have. This thesis aims to combine technical and juridical thought leadership for analyzing possible additions to the current legislation and to the European ICT certification scheme's structure.

The thesis aims to answer the following questions:

1. Does the current European Directive of Network and Information Security (NIS), and the proposed revised directive (NIS2) and the European Cybersecurity Act together, with the official guidelines released by ENISA, form a sufficient layer of mandated cybersecurity protection for connected enterprises and digital infrastructure?

   This thesis analyses the current cybersecurity legislation and possible gaps in mandatory protection of European critical infrastructure enterprises.

   The purpose of this research question is to bring legislators' attention to the possible gaps in current EU cybersecurity protection.

2. How can small OT solution vendors and service providers be made responsible for the cybersecurity of their portfolio offerings without over-bearing their business by the massive size discrepancy of their client enterprises? Many vendors serve clients that are more than hundredfold larger than they are. Can needed cybersecurity requirements be mandated from the enterprise itself, with a new legislative framework that is suggested to be introduced into the new EU legislation?

3. Why does such a legally mandated framework for operational technologies matter?

Digitalization has changed the risk profiles of previously isolated solutions by adding a multi-layer of new structures to enterprises with novel vulnerabilities, connected networks, and complex automated processes that provide societies a wealth of services and products that both physical and economic health strongly depends on. So why does digitalization of enterprises matter? Discrepancies to the continuous delivery of critical services and products is harmful to both individuals and to the collective body of the society. Society's need for a steady supply of energy and water are strongly linked to physical health, while for example some manufacturing are considered vital for economic health. [1]

Digitalization has also changed the fundamental, architectural, and physical structures of critical infrastructure enterprise IT stack and enterprise digital infrastructure. Connected enterprises, their operational technologies and connected infrastructure are tailored to automate tasks and remotely control processes, from factory floor IoT solutions that bring real-time information on to hosted edge computers with added computational power added to the

[1] Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience

processes. Operational technologies of critical infrastructure enterprises and the legislation protecting them are the broad topic discussed in this thesis.

1.3 The purpose of this thesis

The purpose of this thesis is to introduce a new framework to ensure enterprises are taking the necessary steps to protect their operational technologies against cybersecurity incidents and malicious attacks. This thesis combines legal expertise with over decade of hands on work in designing, planning, and leading large digital transformation programs of Fortune 500 enterprises. This thesis aims to introduce additions to the current EU-wide cybersecurity legislation by way of the new mandatory framework required for operational technologies. Features of the framework include mandatory processes and protective measures for IT/OT architecture, security audits, monitoring, and access control. The goal is to inspire for a wider adoption of not only digitalization, but cybernization[2] principles within the European Union. The framework is intended and designed to help enterprises becoming increasingly protected from within.

This thesis' aimed readership includes EU's legislators as well as global IT and legal executives that work with enterprise technologies in leadership positions that are critical for sustaining the European digital infrastructure and critical infrastructure's enterprises.

1.4. Methodology and structure

To address the research questions of the thesis, a legal dogmatic method, also known as legal doctrine, is applied. Dogmatic research has two dimensions or purposes: interpreting the content of existing legislation and systemizing the legislation.[3] In trying to achieve these purposes, the dogmatic method firstly takes a stand on what makes up the existing legislation and secondly how it should be interpreted. Of course, the division is somewhat arbitrary – the two dimensions are intertwined because to determine what makes up the existing legislation one must already interpret its contents.[4]

[2] Tuunanen, et al. (2019)
[3] Aarnio (1997), p. 36-37
[4] Hirvonen (2011), p. 24.

Firstly, the goal of interpreting the content of existing legislation is archived by presenting the existing EU-wide law that governs the cybersecurity of operational technologies. The most relevant legislation being the Directive 2016/11481 on security of network and information systems (the NIS Directive), the Cybersecurity Act (2019), and the yet-to-be implemented Revised Network and Information Security Directive (NIS2). The role of European Union Agency for Network and Information Security (ENISA) is also discussed. Both the existing secondary legislation as well as non-binding principles are considered.

As well as presenting comprehensively the principles, rules, and concepts governing a specific legal area or body, legal dogmatic research also seeks to scrutinize the relationships between these principles, rules, and concepts, with the goal of resolving ambiguities and gaps in the existing legislation.[5] To tackle this second goal (scrutiny), the second part of the thesis consists of presenting the problems of the existing EU law governing the cybersecurity of operational technologies. The legal sources presented earlier will be analyzed, and their combined applicability and combined best practices will be assessed from the viewpoint of how effective they are in legally requiring protective technical measures for fully or partially self-developed operative technologies in order to protect the critical infrastructure of connected, modern enterprises and their extended networks. What is crucial to assess is whether the existing legislation can protect critical infrastructures even when the adopted technologies change, risk levels change, or when the development or adoption of new technologies bring about novel risks.

This thesis also proposes solutions to solve the ambiguities and gaps in the existing legislation. Even though the EU is continuously assessing whether new cybersecurity legislation is needed, it is hard to implement comprehensive legislation, because technologies and the threats they face are ever changing. The theme also falls between two fields: computer science and law. Technical experts are often unable to fully comprehend the complex impacts legislation has in steering development and adoption of novel innovations, all while lawyers often fail to understand the maturity and potential of developing technologies on the European critical infrastructure as they lack technical experience. Therefore, effective frameworks are hard to develop into legislation without experts that have both technical competence and experience in drafting legislation. Rapid development of novel attacks orchestrated through operational

[5] Gestel, Micklitz & Rubin (2017), p. 212.

technologies, IIoT, and other developing technologies, gateways, and our digital infrastructure requires adoption of new legislative tools that have been co-developed by lawyers and technology professionals in unison.

The framework proposed in this thesis is the product of working in the frontiers of digital transformation as a trained legal professional. By combining legal design thinking together with technical expertise, this thesis aims to provide practical suggestions for immediate improvements to the existing EU legislation governing operational technologies. The framework would potentially prevent future gaps in legislation because it would essentially redesign how broader legal principles regarding cybersecurity within critical infrastructure enterprises and the digital infrastructure are introduced by the Commission. The aim is to provide technical requirements to the critical infrastructure's enterprise and network operators to follow.

The thesis is structured as follows: the second chapter is an analysis of the existing European-wide cybersecurity legislation. The roles of the EU Network and Information Security Directive and its revision, EU cybersecurity act, and ENISA's role are discussed and analyzed.

Chapter 3 presents the core design elements of EU digital infrastructure, focusing especially on peaked interest on operational safety and reliability, with both historical and design principles' perspectives. Chapter 4 presents operational technologies and explains the idea of the "fourth industrial revolution".

Chapter 5 introduces the history and discusses how the use of operational technologies have changed over the years from isolated systems into a part of the connected enterprise, and how the change has made operational technologies vulnerable to malicious attacks, as they were not originally designed secure. The chapter also goes over the most common operational technologies solutions.

Chapter 6 explains the concept of operational technologies why they are vulnerable to attacks under the current cybersecurity regulations. In chapter 7 the impact of missing primary and secondary legislation is discussed - the issue of the "lone captain" is presented, ergo the problem

that CIOs face the burden of building secure IT/OT environments alone without the help of EU steering. Chapter 7 also presents sector specific data on cyber related incidents.

Chapter 8 exposes how the most vulnerable solutions of modern, connected enterprise IT/OT environments are excluded from current EU legislation, and how legal maneuvering of IT vendors happens. The chapter builds on the thesis' message of strengthening the security of enterprise operational technologies without financially burdening small vendors. Chapter 9 explains the significance of the proposed new framework, and how it would impact the operational technologies and their security. Chapter 10 proposes a framework that would include operational security into the EU legislation.

Chapter 11 brings light to the shared responsibility business model that is a commonplace practice by IT/OT vendors. Chapter 12 summarizes the proposed new cybersecurity legislation into a quick-to-read brief. Finally, chapter 13 provides an overall conclusion of the thesis.

2 Analysis of existing EU-wide cybersecurity legislations and EU's recent efforts to strengthen Union-wide cybersecurity

2.1 The Network and Information Security Directive

The European Union has taken several measures to develop policies against cyber threats. After all, if not addressed through the appropriate mechanisms, tools and processes, compromised network protection can severely hinder the EU's plans for economic growth embodied in the Europe 2020 strategy, the Digital Agenda for Europe, and the Digital Single Market Strategy. In the Cybersecurity Strategy of the European Union (2013), drastically reducing cyber-attacks, cyber espionage and cybercrime in general featured as a key priority objective.[6]

Directive 2016/11481 on security of network and information systems (the NIS Directive) was the first horizontal legislation undertaken at European Union (EU) level for the protection of network and information systems across the Union. The NIS Directive, published in July 2016, aims to address this need by putting forward "*the measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market*". Even though Directive 2016/11481 was the first horizontal legislation to be enforced, the EU has been tackling cybersecurity issues in a comprehensive manner since 2004, when ENISA (European Union Agency for Network and Information Security),4 a new specialized EU agency, was founded. ENISA's mission is to raise "*awareness of network and information security and to develop and promote a culture of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organizations in the Union*".[7]

About twenty years ago EU discourse slowly started to reflect the idea that societal reliance on technology constituted a rapidly growing security risk that had to be adequately addressed. This conversation was provoked by increasing numbers of cyber-attacks on individuals, companies, and critical infrastructures. Given that cyberspace is not limited by national boundaries, the EU presented itself as the logic and efficient solution to Member States' challenge of how best to tackle cybersecurity threats. This mindset was behind the creation adoption of legal measures,

[6] Christou (2018)
[7] Markopoulou, Papakonstantinoua & Hert (2019)

such as the 2005 Council Framework Decision on Attacks against Information Systems, and the creation of new infrastructures, including the creation of the European Network and Information Security Agency (ENISA) and of the European Cybercrime Centre at Europol (EC3), in 2013.[8]

In terms of legislation, however, the NIS Directive its most ambitious instrument to date, given that it introduces incident reporting obligations for the private sector (for operators of essential services and digital service providers).[9] The directive aims for high-level protection of information systems and networks, aiming to introduce a wider adoption of security elements and improved collaboration and reporting on the Member State and Union levels. The driving force behind the introduction of the new directive is ENISA, European Union's agency for cybersecurity. The directive on security of network and information systems of the European commission clearly brings new member state level network and ICT cybersecurity coordination amongst the Member States. The Directive introduces that Member States should have a minimum country-level capabilities, strategies, policies, and collaboration in information sharing and reporting in place both within their own territory, and as a collective. The minimum level of security for both networks and information systems on the high-level is a great start in protecting the EU's digital infrastructure and connected enterprises through a trickledown effect that the implemented enhanced country-level cyber and network protection organs and processes create.[10]

The NIS Directive consists of 27 articles. The first 6 articles set its scope and main definitions, including the explanation of what constitute as operators of essential services (article 5), as well as the definition of significant disruptive effect (article 6).

The aim of the Network and Information Security Directive is to accomplish "*measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market*".[11]

[8] Carrapico & Barrinha (2018)
[9] Carrapico & Barrinha (2018)
[10] Directive 2016/4811. L192/2 (5)
[11] Directive 2016/1148, Article 1

Articles 7–10 describe the national frameworks that shall be adopted by all Member States on the security of network and information systems. These frameworks include, among others, Member States' obligation to introduce a national strategy and to designate national competent authorities (including a single point of contract and the computer security incident response teams (CSIRTs), as well as, the creation of the Cooperation Group. The Cooperation Group ("CG"), established under article 11, aims to facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them. Article 12 establishes the creation of a network of the national computer security incident response teams' network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation. The articles that follow (14–18) establish security and notification requirements for operators of essential services and for digital service providers (online marketplaces, online search engines and cloud computing service.

However, the current legislation excludes small enterprises from the definition of relevant digital service provider. The adoption of standards and the process of voluntary notification are dealt with in articles 19 and 20. Finally articles 21–27 include the Directive's final provisions.[12]

The NIS Directive, is the first truly European-wide cybersecurity legislation, and a part of a wider push to increase European preparedness and cooperation, the elimination of vulnerabilities and threats, as well as the awareness of the ever increasing threats of the cyberspace, which have steadily increased over the recent years, as attacks are directed towards operators of essential service operators, also known as the enterprises of European critical infrastructure, commonly healthcare[13], water supply[14], energy, digital infrastructure, financial market infrastructure[15], transport, and banking services as outlined in Annex II of the NIS Directive.[16] While taking a closer look at the subsector divisions, electricity[17], oil, gas[18],

[12] Markopoulou, Papakonstantinoua & Hert (2019)
[13] Directive 2011/24/EU
[14] Council Directive 98/83/EC
[15] Regulation (EU) No 575/2013
[16] NIS Directive, Annex II
[17] Directive 2009/72/EC
[18] Directive 2009/73/EC

common modes of transportation[19] and healthcare[20] including both private and public hospitals are defined as OES.

The NIS Directive is aimed towards both DSPs and OES's as well as Member States to manage their cyber security related risks, and in order take into consideration ways to minimize the risk of incidents, as well as require the DSPs and OES's to notify the appointed national authorities that are relevant to the breach of significant breaches, as per the sectors which are referred in Article 2, the services referred in Article 3, and the computer security incident response team, CSIRTs, referred in Articles 1 and 8 of the NIS Directive.[21]

2.2 The revision of the Network and Information Security Directive

The EU is constantly increasing and updating existing legislation. In December 2020, the European Commission proposed a revised Network and Information Security Directive (NIS2) to replace the 2016 Directive.[22] The new proposal responds to the changing threat environment and takes into account the digitalization of our society, which has been accelerated by the coronavirus crisis. The key objectives of the NIS2 directive include tightening up companies' security obligations, addressing supply chain security, introducing stricter control measures for national authorities, and further increase information exchange and cooperation. The proposal is currently being discussed in the Council.[23]

NIS2 is a revised legal instrument that requires Operators of Essential Services (OES) and Digital Service Providers (DSP) to adopt risk management practices, and without delay notify incidents to national authorities. The NIS2 did strengthen the security requirements with incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption. Streamlined incident reporting obligations with more precise provisions on the reporting process, content, and timeline for the large vendors and national authorities. Accountability of malice or negligence regarding to enterprise's management of legally required compliance with cybersecurity risk-management measures is

[19] Regulation (EC) No 300/2008; Regulation (EU) No 1315/2013; Directive 2012/34/EU; Regulation (EC) No 725/2004; (EU) 2015/962
[20] Directive 2011/24/EU
[21] NIS Directive, Articles 1, 2, 3, & 8
[22] Directive 2016/11481
[23] European Commission 2021a

included in NIS2. The revised NIS2 Directive did not bring a needed change, and continued to leave small vendor technologies outside of its scope due to unfair burden of financial costs mandatory audits, monitoring, and the other responsibilities large digital service providers have to follow would cause .[24]

The revised NIS2 Directive, the EU-wide cybersecurity law, excludes small and medium digital service providers (DSPs) outside of the scope of it, which is the core reason why this thesis was written. "*To avoid imposing a disproportionate financial and administrative burden on operators of essential services and digital service providers, the requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. In the case of digital service providers, those requirements should not apply to micro- and small enterprises*."[25] Understandably, finding the sweet spot in balancing between imposing security related financial responsibilities and encouraging adoption of solutions and speeding digitalization is anything but straightforward. Regardless, this thesis wants to bring light to the current vulnerabilities that exists in connected enterprises, especially regarding operational technologies, as well as the issues in how current EU-wide cybersecurity legislation is built.

Unfortunately, the NIS2 Directive takes a very clear and strong stand on enterprise security in Article 16 by scoping out small service providers: as they are not in the volume business such as the likes of Microsoft, they cannot take the responsibility of cyber related risks of the enterprises they sell their services or operational technologies solutions to. Instead, they have either managed to contractually divide their portfolio of services into subcontracts and distributed model of serving large clients, or they are simply out scoped by their small size. The size of the companies that provide the solutions for Fortune 500 enterprises manufacturing and service delivery operations are typically hundredfold smaller than their clients. Unfortunately, contractual maneuvering happens, which takes the burden of taking the legal responsibility of cybersecurity incident responses off the shoulders of the enterprises as well.

The service contracts are engineered in a way that all security-related responsibility is lifted from both the enterprise that purchases the solution or the co-development of it, and the provider

[24] NIS2 Directive, Chapter 13
[25] Directive (EU) 2016/1148 (53)

of such service and/or its development and support services for solution that are traditionally co-developed or self-developed by enterprises own IT workers and the small vendors that provide them. Such contracts are a commonplace. The impact of removing the liability from the provider and the enterprise in case of a major cybersecurity incident. Incase OT solutions are the reason, the enterprise's insurance company pays for the damages, without questioning the actual degree of monitoring and protective measures that have been in place to prevent and minimize the impact of potential risk of incidents.

The avoidance of responsibility by legal maneuvering with the service contracts and the current loophole in EU cybersecurity law translates directly to diminishing responsibilities. Contractual cybersecurity related risk management tactics have for long been a commonplace practice in the IT industry; it is one of the favorite plays of the IT industry service and solution providers that either sell their own or a third-party's solutions or services.

2.3 The Cybersecurity Act

In addition to the implementation of Directive 2016/11481, the EU has introduced a new Cybersecurity Act (implemented in 2019), that

1) with Article 48.2, strengthens the role and power of ENISA by giving it a permanent mandate and more resources and new tasks. By authority of the Cybersecurity Act, ENISA now has a key role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes. It is in charge of informing the public on the certification schemes and the issued certificates through a dedicated website. In the Act, ENISA was also mandated to increase operational cooperation at EU level, helping EU Member States who wish to request it to handle their cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross- border cyberattacks and crises. This task builds on ENISA's role as secretariat of the national Computer Security Incidents Response Teams (CSIRTs) Network, established by the Directive on security of network and information systems (NIS Directive).[26]

[26] European Commission 2021b

2) Introduces a unified set of certification standards that bring Europe's cybersecurity towards a common level of maturity. The Cybersecurity Act establishes an EU cybersecurity certification framework which will allow the emergence of certification schemes for specific categories of ICT products, processes and services. The act aims to bridge previously regional and national certification efforts into an EU-wide cybersecurity strategy for IT solutions. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognized across the European Union. The European Union has introduced many new ideas to introduce collaboration among member countries as part of the steering strategies Europe's Digital Decade[27] and Single Digital Market.[28] The EU Cybersecurity Act can be considered a major step forward towards the creation of a single European market for cybersecurity products and services.

The future cybersecurity certification scheme developed by ENISA with the mandate of the Cybersecurity Act must achieve a number of cybersecurity objectives, which are aligned with established best practices. The key objectives of the act strive for the future framework to include:

1) Information security: To protect data against accidental or unauthorized processing, access, disclosure, destruction, storage, loss, alteration or lack of availability during the entire lifecycle of the ICT product, service or process.

2) Access control: That authorized persons, programs or machines are able to access only the data, services or functions to which their access rights refer.

3) Vulnerability assessment: To verify that ICT products, services and processes do not contain known vulnerabilities.

[27] European Commission 2020c
[28] European Commission 2020d

4) User activity monitoring: To record and make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom.

5) Cyber resilience: To restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident.

6) Security by design: That ICT products, services and processes are secure by design and by default.

7) Patch management: That ICT products, services and processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities and are provided with mechanisms for secure updates.

The future certification that European Cybersecurity Act tries to take into action in the coming years, takes clear steps toward standardization of cybersecurity measures. "Modern ICT products and systems often integrate and rely on one or more third-party technologies and components such as software modules, libraries or application programming interfaces. This reliance, which is referred to as a 'dependency', could pose additional cybersecurity risks as vulnerabilities found in third-party components could also affect the security of the ICT products, ICT services and ICT processes. In many cases, identifying and documenting such dependencies enables end users of ICT products, ICT services and ICT processes to improve their cybersecurity risk management activities by improving, for example, users' cybersecurity vulnerability management and remediation procedures."[29] The aspired themes that a future EU cybersecurity certification framework models within it seem very similar to, and therefore could almost directly model after the most common US-based, yet globally recognized ISO certification schemes. One of the key difference would be that since cybersecurity is becoming increasingly prominent and necessary, it is important for quality assurance and security reasons to have an official European standard for certifications, just like the CE conformity marking,

[29] Regulation (EU) 2019/881

which proves that a manufacturer or an importer conforms that the product or service is up to European environmental, safety, and health protection standards.

In Article 8 of the Cybersecurity Act, ENISA is given the mandate to support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, as established in Title III of this Regulation by monitoring developments, on an ongoing basis, in related areas of standardization and recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to point where European standards are not available, and preparing candidate European cybersecurity certification schemes for ICT products, ICT services and ICT processes.[30] The v1.1.1 of the candidate certification is not yet in distribution, but since the implementation of the Cybersecurity Act, ENISA has already begun the work towards replacing SOG-IS with a modern candidate cybersecurity certification scheme EUCC.[31] Cybersecurity as a core strategic initiative is strongly pushed at the frontier of Digital Single Market and the recently introduced Digital Europe Programme – a 1.9 billion euro program that runs from 2021 until 2027. These efforts from the European Union and ENISA; like the publishing of the Digital Europe Programme, speaks volumes of how truly important it is to begin mending the vulnerabilities in European connected enterprises and digital infrastructure so that we can have strong and secure pillars that our developing digital infrastructure is being built on. Future's European cybersecurity is being made today. Security as a strategic core element needs to be implemented now for critical infrastructure enterprises across sectors, in order to secure reliable performance and operational safety, which also is why ENISA was authorized in the Cybersecurity Act to mandate more action from Member States in terms of their collaboration and efforts in take care of cybersecurity within the nations.[32]

2.4 ENISA's role

The strengthening of ENISA's position (by mandate of the 2019 Cybersecurity Act), and therefore making the steering documentation published by the office brings momentum to the adoption of recommended practices. There is a clear difference between mandatory and

[30] Regulation (EU) 2019/881
[31] ENISA Candidate Scheme V1.1.1 (2021)
[32] European Commission Cybersecurity Policies

enforceable certifications. Our current legislation underperforms in defining legally binding requirements in upholding necessary security measures that our critical infrastructure and the operations our societies depend on. These requirements are often discussed in ENISA publications and industry recommendation pieces, but as long as there are no mandatory European frameworks designed to the needs of our Digital Infrastructure members, to steer enterprises, it will be hard to say that Europe has done all it can to ensure the future Single Digital Market.[33]

In addition to ENISA, the European Union organizes semi-official events, hosts webinars, and releases working session memos and papers in co-operation with the European Union Institute of Security Studies (EUISS). The institute acts as a center agency assessing foreign, security and defense policy issues. The EUISS organization strongly relies on the European Common Foreign and Security Policy, which is documentation of mutual commitment to protecting the Union through NATO, the North Atlantic Treaty Organization.[34] The published documents center cybersecurity and defense against offensive attacks, especially those that are aimed towards the European critical infrastructure. ENISA and EUISS together aim to assist Member States in requiring their infrastructure member organizations prepare for, and improve resilience and security measures against malice large-scale cyber-attacks and disruptors.[35]

2.5 The existing gap between current EU cybersecurity legislation and ENISA

The power and importance of enterprises has grown to an unseen magnitude and role in our digital societies. The current legislative frameworks and the role of ENISA leaves a significant gap between mandated requirements and what are often called as industry best practices or ENISA's recommendations. This thesis introduces a framework that can help in bridging the current gap between ENISA's industry standard best practices and mandated protective measures in European Union's legislation. With the introduced framework, adaptation of protective measures and ensuring sufficient monitoring would no longer be optional to have in place. Such framework indirectly would impact both European economic and human safety, as

[33] ENISA Strategy 2020
[34] Common Foreign and Security Policy (CFSP)
[35] EUISS (2020)

our digital infrastructure and networks would be less vulnerable to hostile attacks, safety increases.

Enhanced State-level protective measures trickles down to indirectly protecting enterprises, but as secondary legislation, it is not enough to keep EU's enterprises safe. This thesis explains what types of elements to include in a future secondary legislation. The proposed framework aims to have elements that stay relevant regardless of the leaps offensive and defensive technologies take. It is defined to be a practical legislative tool to unify connected enterprises cyber protection and support single organizations' abilities by providing a minimum set of elements to uphold, instead of relying solely on the discretion of the CIO or CISOs team on overseeing multi- national enterprise's security across all elements.

The NIS2 Directive uses two terms for different types of enterprises and sets requirements for them: They are Digital Service Providers (DSP) and Operators of Essential Services. Digital Service Providers are large platforms and providers that play a very significant roles in service continuity in Europe. The top term is divided to three sub-terms, as their importance on ensuring continuity is rightfully noted in the legislation. The mentioned sub-DSPs are online marketplaces, search engines, and cloud computing resources. The latter represents the infrastructure and the backbone or even skeleton of IT industry playmakers; the services that utilize cloud computing resources enable access to a shareable asset, for example to cloud-based hybrid environments that hosts business critical applications and service infrastructure, that makes our connected enterprises work. Enterprises are becoming increasingly dependent on cloud computing resources, and without them working, infrastructures across sectors could be paralyzed. The other mentioned term is OES, Operator of essential service. OES's include energy industry, transportation, financial, health, drinking water, digital infrastructure, and banking services enterprises.

ENISA, together with NIS and the proposed revised directive (NIS2 Directive, and through the introduction of other practical tools and organizational cooperation are growing the cybersecurity culture in Europe. Examples include the establishment of the cooperation and information exchange group with through an established Computer Security and Incident Response Team CSIRT, and by providing the NIS Toolkit, in addition to the European Cyber crises liaison organization network (EU- CyCLONe) to oversees responses large-scale

cybersecurity attacks. The measures are aiming to increase the awareness and provide tools for both enterprises and Member States to unify protection of essential services and helping DSPs and OES's by promoting the global security stables; ISO27001, ISO27035, ISO22301 certificates, as they can be ideal framework for large digital service providers and operators of essential services.[36] The ISO 27001 is a globally recognized certificate scheme, that establishes compliance with cyber security best practices for data and IT asset management. The certificate is a commonplace for most large Digital Service Providers, defined as online marketplaces, online search engines and cloud computing services[37].

ENISA has published a document called Technical Guidelines for the implementation of minimum-security measures for Digital Service Providers. The document outscores OT providers and OT technologies outside of it, by including DSP providers, in this context meaning platform technologies and therefore most adopted enterprise software solutions and their respective globally recognized and operating providers. The exact list of in-scope providers includes Infrastructure as a Service providers, Platform as a Service providers, Software as a Service providers, and Internet Protocol providers; or in other words, the giants, as stated in recital 57. EU legislation does not include small OT solution providers, as they are clearly out scoped from the NIS Directive, as stated in Article 16. This issue is the very reason of this thesis. Since the definition includes only DSPs that are defined in the NIS Directive as any legal persons that provides digital services at scale, as described in Annex III of the Directive, and Operators of essential service providers (in this context meaning critical infrastructure networks). The European Union leaves the work of defining requirements and monitoring the market onto Member States organizations and their respective efforts at creating national cybersecurity laws. This causes discrepancies in the maturity and adoption of national cybersecurity legislations among Member States, which leads to going against the principles outlined in European Single Digital Market strategic initiative. While some Member States aim to cover the loopholes and openings left behind by the EU NIS Directive, it is difficult even with the required competent authorities and notification requirements in place. The Member State requirements seem to lean towards post-incident responses, instead of requiring

[36] IT Governance
[37] NIS2 Directive, Annex III

enterprises to protect and monitor the complete of their IT environments, with operational technologies being included.

Unfortunately, most countries do not have information and cybersecurity legislation with minimum safety and security requirements for small and medium size IT and OT solution providers, and by allowing the burden to be on Member States, the EU is falling helplessly short of ensuring that there would be unified Single Digital Market in terms of Unified Cybersecurity and Information Security Directives. The potential harm caused to critical infrastructure is alarming, and without the inclusion of minimum requirements for small enterprises to organize monitoring and regular audits of the OT solutions that they use, and without enforceable punitive measures in case said small enterprises would not comply with the minimum requirements, EU's attempts to build a reasonably sound preparedness against offensive threats will not become a reality anytime soon.[38]

ENISA keeps up with all types of known offensive cybersecurity attacks and vectors on modern technologies. They advise primarily governments, but at request also enterprises, in developing zero-day responses and enhancement of protective measures of connected networks and digital infrastructure, ICT infrastructure, and enterprise IT infrastructure. Narendra and Singh (2020) introduce a metric value of attack, based on ENISA's recognized cloud-technologies related possible risks with their connected and related taxonomies. These types of works are often easily disregarded, but are vital for the unified Digital Single Market, and therefore ENISA as an organization. Cybersecurity community's efforts to unify language and modeling that is used in risk assessments and reports are advancing cybersecurity preparedness in the Union, even without having legislative power behind them, thanks to the willingness to adopt work that the community publishes in order to advance the industry.[39]

[38] Cadler (2018)
[39] Narendra & Singh (2020)

3 Core design elements of the European digital infrastructure

3.1 The pillars of industrial and operational design

Europe's critical infrastructure's overall industrial and operational designs were created with reliable performance and operational safety as their core design elements. The pillars of industrial and operational design elements that infrastructure has been and continues to be built on were created during the first and second industrial revolution. These core design elements, that include both the operational and physical components, were slowly developed since they were first introduced in the mid-1700s.[40]

The fundamental ways enterprise operations, physical buildings, manufacturing factories, supply chains, and other have developed over the years, but have not fundamentally been redesigned during the third and fourth industrial revolution's digital transformation, leaving integral design weaknesses within them as things have progressively and rapidly become increasingly connected and intelligent. Now, as facilities, operations, machinery, processes, networks, and integrated intelligence in Industrial IoT has connected our enterprises in unseen ways; these technologies have been built, in a way that I one can only describe as a layer, on top of legacy and tradition; on top of core design elements that have existed since the first and second industrial revolutions.

3.2 Security as a core design element of a connected enterprise

Safe operation, reliable performance, and security of these key assets are essential to public health, economic security, and national safety. Outside stressors, especially novel cyber-attacks, pose a serious threat to our physical and digital infrastructures, lives, environment, and our sovereignty, as they have the ability and the power to cripple our critical infrastructure. The European critical infrastructure was built before an era of minimal outside stressors; the

[40] OECD (2015)

foundations did not include the fundamental security element, excluding the most obvious physical security measures.[41]

Security as an element of strategy in critical infrastructure industries was widely introduced in civil nuclear industry plants' in the West. The core strategic drivers in critical infrastructure industries were originally safety in internal operations and usage, and reliability in terms of minimizing unplanned stoppages. Industries were designed with operational safety and reliability in mind, to avoid internal operation-related mistakes and unplanned stoppages in delivery.

Resources industries first began adopting security as a strategic core design element in terms of internal and operational safety prominently in the 1970s, when the energy sector's civil nuclear plants began operating globally. The first real black swans, which were unaccounted for and unplanned for in terms of possible crisis, happened in massive-scale largely due to operational failures and fragility, not due to malice external attacks. Reasons leading to the first civil nuclear crisis were largely due to lack of documentation of internal processes and design flaws in operations. The nuclear disasters caused lasting and extensive harm to humans and the environment, which in its own was enough to heighten the emphasis and corrective action in securing plants internally after governments launched investigations, plant improvements, and other self-corrective measures. Actions were taken within the industry itself, as nuclear scientists came together for knowledge transfer by arranging first industry conferences assisted each other in developing universal basis for security measures for plants.

[41] European Central Bank (2016)

4 The development of operational technologies through the four industrial revolutions

The industrial revolution of the 18th century was famously invoked by a step up in technology. Industries which had traditionally relied on work by hand started to embrace a new future of machine use to dramatically enhance output levels, efficiency, and financial return.

Comparatively, the twenty-first century has seen a similar revolution, particularly in critical national infrastructure and manufacturing industries, where Information Technology (IT) has been and is increasingly being used to control, maintain, and modify their output. With our reliance on Operational Technology (OT) increasing and their levels of IT connectivity growing, with the security of service being imperative to maintain availability.

As businesses require access to real-time operational data, their OT systems, which were previously isolated and secure, are increasingly being connected to corporate networks and the Internet. While the interoperability of OT and IT opens a whole new world of opportunities, it also opens the door to unaddressed cybersecurity risks in OT environments.[42]

This OT and IT interoperability is quickly evolving into the Industrial Internet of Things (IIoT). This convergence of OT and the Internet of Things (IoT) is characterized by the utilization of machine learning, big data, sensors, and machine-to-machine communication in industrial settings. IIoT is the primary force behind what's being called the fourth industrial revolution or Industry 4.0, which is the creation of 'smart factories' that combine cyber-physical systems, the IoT, and cloud computing.

With each additional step towards further automation and interconnection there is an increase of exposure to cyber risk. Furthermore, in an industrial environment, cyber incidents can quickly escalate into physical damage to equipment, injury, or loss of human life.[43]

[42] Galinec et al. (2017)
[43] Benincasa (2021)

5 Enterprise operational technologies

5.1 Operational technologies and industrial control systems

Operational Technology (OT) systems were traditionally only designed for the purpose of local control and to be reliable and safe rather than secure. However, most of these systems are now connected to either an enterprise network or via the internet for remote operations. Commercial off the shelf software and general-purpose hardware are also being used to replace proprietary OT systems. This means security vulnerabilities affecting those technologies can now be exploited in OT environments without specific knowledge of OT systems.[44] The systems are then made even more insecure because many of the standard cybersecurity protection measures normally used with these technologies have not been adopted in the OT environment.

Early networks in industrial and enterprise settings consisted of hardware with the ability of computing basic and simple tasks while being connected within a closed network of a single central server with terminals[45] in a localized location, usually the building complex itself. These closed networks of localized computers were quickly transformed with the commercial software and hardware, as well as the internet service provided by telecom companies. In the late 1980s software companies began rollouts of software that was tailored for specific industrial use, called Operational Technologies OT and Industrial Control Systems (ICS).

Operational technologies are software and hardware solutions designed to reliably run and locally control highly specific processes and tasks. Operational technologies began as, as all digital assets, fully proprietary technologies and solutions, but since commercial stack technologies[46] have begun increasingly commercially available, off the shelf solutions and partially tailored solutions have become commonly used within the critical infrastructure.

[44] Galinec et al. (2017)
[45] Terminals have screens and keyboards, but they do not necessarily include a server with computational power within themselves
[46] A technology stack, also called a solutions stack, technology infrastructure, or a data ecosystem, is a list of all the technology services used to build and run one single application. The social site Facebook, for example, is composed of a combination of coding frameworks and languages including JavaScript, HTML, CSS, PHP, and ReactJS. This is Facebook's 'tech stack"

Historically, as operational technologies solutions were separated from enterprise IT infrastructure, the threats associated with the enterprise IT environment did not reach the isolated operational technologies layer closest to the core production or service of the enterprise. As Conklin (2016) writes, "*Ten years ago, to get to most OT systems involved air gaps, leased lines and dedicated serial circuits. Today the network connectivity is via TCP/IP and over the Internet*." Cybersecurity processes like security monitoring, audits, access control, and protective solutions within the connected IT infrastructure, like whitelisting encrypted firewalls, and other modern network security technology protective measures are needed, but OT solutions have the standing problem; they were not designed with security as one of the core design elements due to their original isolated environment. Conklin (2016) continues "*History has shown that the effectiveness of these solutions is far from perfect, in fact in recent testimony, the director of the NSA gave critical infrastructures an average score of 3 out of 10 for level of security protection, with 10 being the highest level possible*".[47]

As the original usage of these programs was strictly running and controlling localized single processes, security was not considered a core design principle of the solutions. Same fundamental security issues remain nowadays, when our enterprises are highly connected; operational technologies used by the critical infrastructure are now assets connected into networks, increasingly managed remotely with shared responsibilities for different parts of the solution services and their management, and most alarmingly for this thesis – are without any legally mandated documentation, processes, or audits in place to ensure safety and security. There is an urgent need for legislation that would call for a party to be responsible for arranging all of the necessary processes and documentation in place.

Critical infrastructure's operational technologies that include industrial control systems are proprietary technologies or tailored, making them less likely to have sufficient and continuously updated cybersecurity protection measures that commonplace solutions have, which considerably increases the risk of security vulnerabilities in the age of increasingly sophisticated attacks toward both physical and digital infrastructure.[48] Closed networks used to

[47] Conklin (2016)
[48] Hemsley & Fisher (2018)

hold a limited amount of servers that ran operational technologies with a limited amount of terminals and even smaller group of actors that had a granted right to operate such systems.

Networks are becoming increasingly complex, next-generation environments[49] with digital infrastructure providing possibilities for remote and centralized control of different functions and physical assets of a connected enterprise.[50] The first networks (LANs) were closed environments that connected single computing systems that ran a limited amount of operational technologies on a server, often also limited physically to one site like a plant or a facility. Nowadays most networks outside the most high-security facilities like nuclear plants are connected to the internet. While connectivity increases, so does the sheer volume of process-related data transmitted also in industrial and manufacturing context, which makes the importance of all data being encrypted instrumental in ensuring end-to-end protection in a connected enterprise. Closed networks have naturally less complexity, which impacts both the risk profiles and the necessary steps that are needed for appropriate technical processes, data protection, and access management protocols.

5.2 The purpose of operational technologies

5.2.1 The most common operational technologies systems, listed per purpose

- Process Automation Systems (PAS)
- Industrial Control Systems (ICS)
- Integrated Administration and Control Systems (IACS)
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control Systems (DCS)

[49] A shift to next-generation environments has created a new category: software-defined security. An example of network functions virtualization (NFV), software-defined security provides a new way to design, deploy, and manage networking services by decoupling the network function from hardware appliances. Created to consolidate and deliver networking components necessary to support a virtualized infrastructure, software-defined security includes virtual servers, storage, and even other networks.
[50] Nicholson et al. (2012)

- Process Control Network (PCN)
- Process Control Domain (PCD)
- Manufacturing System
- Critical National Infrastructure (CNI)
- Safety Instrumented System (SIS)

These are specific purpose serving solutions that are predictable in their function, the data they require, and the data that gets extracted from the process itself. They are close to the core function of the enterprise itself: manufacturing process and factory floor solutions are typical examples of OT use cases.[51]

[51] Iaiani, et al. (2021)

6 Operational technologies and security

6.1 Connected operational technologies are a recognized vulnerability

Operational Technology (OT) are systems that were traditionally designed to serve a single purpose that is directly related to enterprise core business operations; manufacturing or producing of a service. OT had centralized. local control and they were designed to be reliable and safe to operate, rather than secure. However, most of these systems are now connected to either an enterprise network or via the internet for remote operations. Commercial off the shelf software and general-purpose hardware are also being used to replace proprietary OT systems.

Connected operational and process systems, some that have been developed for a specific task, and that have been in production for decades, are a part of developing digital environment, with an ever-connected nature, and management. With enterprise technology stack being increasingly connected, the operational technologies solutions meant to work in isolation, are being connected to a wider infrastructure and multitude of business systems, production solutions, and core enterprise operations solutions. As Caldwell writes (2018) that "*the integration of systems that have traditionally run machinery as standalone, closed-in operations with the Internet has created both an opportunity and a challenge*."[52] This creates big data flow from and to operational technologies solutions, which can significantly improve operational efficiency and performance while measuring output quality. Modern enterprises with legacy operational technologies solutions are increasingly digitizing their IT infrastructure around their OT solutions, which originally were developed as lone-standing and isolated solutions. The increase in data flow and degree of digitalization of core operations are changing the environment that surrounds the legacy operational technologies, which may make the previously isolated and now-connected solutions the weakest link in the connected enterprise IT environment.

6.2 Thinking outside the box with monitoring and security operations setup

Networks can be an option for not only connect OT systems into the wider IT environment of

[52] Caldwell (2018)

the enterprise, but also be a point of security that protects OT. Since most monitoring meant to scan IT software solutions and the networks themselves could break an OT solution, monitoring network and APIs that face OT solutions could be used as a mandatory secondary protective layer against OT hacks and offensive attacks, - anomaly or suspicious traffic can be detected by network scans, even when they're not network specific, but rather OT specific anomalies; algorithm flags what it's programmed to flag.[53]

Information security is needed as a consideration in public procurement of ICT solutions, as well as a design principle in enterprises' purchasing decisions when selecting new IT solutions. The weight of information security is trumped currently by functionality and usability in valuation processes.[54] The issue of replacing legacy solutions, and developing existing ones needs additional work on information security.

This means security vulnerabilities affecting those technologies can now be exploited in OT environments without specific knowledge of OT systems.[55] The systems are then made even more insecure because several of the standard cybersecurity protection measures normally used with these technologies have not been adopted in the OT environment.[56]

6.3 Operational technologies vulnerabilities: Identification, Protection, Detection, and Response

- Identify: Identify the current OT landscape to design specific protection measures to prevent a cyber-attack against OT systems commensurate to the business risk

- Protect: Deploy specific protection measures to prevent a cyber-attack against OT systems commensurate to the business risk

- Detect: Establish mechanisms for identifying actual or suspected attacks

- Respond: Undertake appropriate action in response to confirmed security incidents against OT systems.[57]

[53] Gomez (2019)
[54] Hale & Greg (2020)
[55] Galinec et al. (2017)
[56] Iaiani, et al. (2021)
[57] Cherdantseva et al. (2016); Galinec et al. (2017)

6.4 Central monitoring

Gosine (2017) discusses the wide-adopted monitoring and security centers and platforms, an ideology of utilizing a Centre of Excellence as a central body dedicated for monitoring and incident response a centralized monitoring as a solution for some IT security. Such platforms and security monitoring centers are a commonplace in enterprises, but unfortunately, they almost always out scope operational technologies from within the overall IT infrastructure's controls and security monitoring.

The large software providers with systemic patching, security updates, and monetary incentives to keep up with vendor-provided security action are the systems that have monitoring provided for them or organized by enterprises. SOC centers unfortunately do not work for small operational technologies solutions with unique purpose and build, and therefore is not an adequate solution to fix the gap and presented issues of this thesis: an additional solution and legislative direction must be present in order to protect operational technologies, even when the overall security is strengthened when IT environments are monitored in a wider context. SOC centers enhance network and connected system security, and in some degree can impact the security of operation technologies solutions that are close to the factory floor or enterprise's business processes by detecting anomality's in surrounding operational technologies and network that may come from or impact connected operational technologies solutions.[58]

In most cases, if the stack OT technology is provided by one of the large providers, information on found vulnerabilities, patching, and security audits are more commonly received. Anton S., et.at (2021) wrote that "*The results of this analysis provide insight about the types of attacks commonly used that PLCs are susceptible to, as well as an overview of the likelihood these PLCs are connected to the Internet.*[59] *This information can aid operators to assess the likelihood and type of attack the OT environment could fall prey to, and aid in implementing counter measures. Furthermore, this analysis provides a methodology for operators to assess the attack surface of their OT environments*." Receiving assistance from the vendors is extremely rare from small OT solution providers, nor is it a commonplace when the enterprise

[58] Gosine (2017)
[59] Anton et.al. (2021)

has co-developed or self-developed OT solutions in use. They simply do not have the resources to deliver needed support, and therefore the enterprise using the solutions should have the legal responsibility of either implementing the framework proposed in this thesis or outsourcing the implementation as a service from external service providers.

7 The impact of the missing EU-wide legislation for enterprise operational technologies

Currently, the design of IT systems, networks, and cybersecurity across the connected enterprise from devices to legacy systems as the protective elements of a connected enterprise, are left to the discretion of the CIO and his team, including sometimes a CISO, to build and maintain a continuously protected connected enterprise. The wider complex infrastructure of IT and OT solutions and networks is currently no one's responsibility in the eyes of EU law. The proposed revised directive (NIS2) does strengthen the security requirements for large digital service providers, and even outlines fines for neglected reporting. The accountability requirements for preventive action and reporting have some sector specific variations, but the enterprise's management of legally required compliance with cybersecurity risk-management measures is included in Article 14 and 16 of the NIS2.

The proposed revised NIS2 Directive's Article 16 has several clauses that needs to be pointed out, for in the context of operational technologies and the rapid leaps of digitalization within enterprises, they NIS2 Directive is not sufficient in protecting a modern, connected enterprise's regarding the enterprise's responsibility over their own IT/OT infrastructure and networks: "*The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph*", as outlined in Article 16.[60]

This EU cyberlaw applies to vendors and service providers that are significant in size, and most of the Big Tech providers, if not all, have ISO certificates in place, which are certificate schemes with the aim of displaying that the holder organizations go far beyond the current EU law requirements in order to provide services and solutions that are built on the principle of security as their core design element.

Old legacy operational technologies solutions that are attached to the production floor or support the core operations are out scoped from the reach of this Directive, but Article 16 further draws for division between co-developed solutions, or for example complex platforms

[60] NIS2 Directive

and outsourced cloud-based infrastructure within multi-vendor environments. Unfortunately, the way this law is designed, it simply does not serve modern organizations, with multitude of vendors and plentiful of small solution providers, co-developers, open-source solutions, and legacy solutions, all of which could be a part and responsible for the most mission-critical production of services and products.

The supervision and legislation of enterprise cybersecurity protection should be for the stringent by giving both ENISA and the Commission legal supervisory mechanisms through mandatory audits of the physical industrial infrastructure and the proposed framework elements.

The EU Network and Information Security steers national law, and the adoption of cooperative measures to create increased dialogue among Member States, which entities are subject to obligations of guarding the scared of network and information system but governing the framework of enterprises should be primary legislation where punitive reinforcement is outlined that any staff should have as supervisory institution the right to audit that the enterprises follow and have adequate measures in place regarding the frameworks elements for discharge and physical safety both internally and externally.[61] Unfortunately, there are no implication or a framework that would steer the whole of the

Current legislation does not reflect the continuously increasing need for a set technical framework that aligns a legally backed minimum set of standards, obligations, and sanctions, for upholding encryption and protection of connected systems in enterprises that are a part of the critical infrastructure. At the EU level, insufficient progress has been made in terms of countering institutional fragmentation, advancing towards binding legal norms, defining what should be understood as resilience and how it should be achieved and appropriate levels of funding.[62] The introduction of such a framework would strengthen and unify preventive protective action across the European Union. In practice, the framework must be designed to be flexible, in order for it to keep up with digitalization. Practically, the framework would include both a minimum set of criteria of protective measures in place, accompanied with mandatory auditing that continues to provide visibility for both officials and the organization

[61] Moreno et al. (2018)
[62] Carrapico & Barrinha, (2018)

itself of the level of protection over time. Currently the burden executing a well-managed enterprise security office lies on the shoulders of enterprises' CIO, CISO and their team members responsible for data security, most often data controllers and enterprises data protection officers. Solor (2020), an Israeli Engineering and security operations expert recommends setting roles and responsibilities for staff, written down operations, and identifying threats and vulnerabilities.[63]

Operational technologies that were developed as isolated solutions running core operations are nowadays a part of a connected enterprise IT and complex networks. The issue relies within they were not developed with security as one of their core design elements. Maintaining strategies and policies relies is on the competence and discretion of the security personnel that are responsible of the OT, as no legally required framework exists. Without a framework to guide policies and action according to the complexity, risk profile, and significance of solutions, structured, effective, and unified protection is not a reality. Data controllers seem to be the only enterprise IT staff members with guiding EU-law that sets structured minimum requirements and processes, mandated by the General Data Protection Regulation. They have a process in place for benchmarking and for guidance. Wright et. al. writes: "*Data controllers may also need to be aware of varying legal requirements in privacy and breach notification laws but also other types of laws as well. For instance, there might be laws that address particular types of information (e.g., financial or employment), cybersecurity and national security*."[64]

The Commission has shown, that newly introduced EU laws such as the Whistleblow Directive and the General Data Protection Regulation are changing how EU law is responding to the rapidly developing digital infrastructure and its' enterprises in Europe. The Whistleblow Directive and the General Data Protection Directive both are drafted to directly require action from technology giants, instead of only requiring national bodies and Member States themselves to introduce national legislation and processes in place. The impact therefore is also intended to reach all the way to individual enterprises, not only through national law; unfortunately placing the burden of the mentioned "requirements" on Member States only distorts the European Single Digital Market and leaves possibilities to gaps to develop onto the EU-wide security legislation and protective measures that are mandated by law. It would be

[63] Solor (2020)
[64] Wright & Hert (2016)

recommendable that the EU-wide cybersecurity, information security, and network security policies would be amended, and the future legislation designed in a dissimilar fashion, and make them target enterprises directly.[65]

The greatly influential and powerful IaaS, PaaS, and SaaS DSP's demand direct control on the European level, and the trend in new and upcoming legislation surrounding data, digital service providers, and workers' rights are that the technology giants are beginning to be subjected to stricter rules and regulation. The European Union should take the next step in protecting the modern, connected enterprises by introducing new EU law that builds on similar legal design elements, and requires critical infrastructure enterprises to have the proposed framework elements in place for their operational technologies, to avoid leaving the current vulnerabilities open for possible offensive attacks. Anton S. et.al. (2021) discovered during their research conducted for their published article The Global State of Security in Industrial Control Systems: An Empirical Analysis of Vulnerabilities around the World published in the IEEE Internet of Things Journal, included over 13,000 operational technologies solutions, that no longer were isolated but connected to the Internet, almost all contained at least one vulnerability. The results clearly stated that European and Northern American enterprises were the most represented in the findings. It is crucial, that the European Union passes EU law that requires enterprises themselves to take action to protect their connected enterprises weakest link; the partially or fully self-developed OT solutions that receive no support from a vendor, and that currently fall outside the scope of current certifications and cybersecurity legislations.[66]

The current EU legislation excludes operational technologies vendors by size as operational technologies solution and service providers are often by size of the organization itself, small, because their business cater for only a very specific purpose solutions and clients, which makes them very different from large IT providers that have easily scalable business. A new EU law is needed that includes operational technologies in its scope, as the nature of OT has changed very dramatically, from being isolated solutions, to being connected to the Internet and the surrounding emprises connected networks and IT infrastructure. The current EU legislation relies on Member States to regulate cybersecurity issues through national law instead of directly requiring action from enterprises, which is a poor strategy considering the Single Digital Market

[65] Whistleblow Directive (EU) 2019/1937
[66] Anton et.al. (2021)

is an important initiative with an aim to secure and unify European IT infrastructure and European cybersecurity.

This thesis recognizes the recent positive adjustments to how newly introduced EU legislation is designed in ways that better serve the aspired Single Digital Market[67], and encourages similar structuring for cybersecurity legislation as the EU has conducted in the new Whistleblower Directive; requirements and possible sanctions are directed towards both enterprises and at Member States, instead of trusting that Member States collaboration and decision to draft national law to involve requirements that are directed at enterprises would and could build on the Single Digital Market strategy's principles. Differing national law is problematic, as the nature of the European Digital Market's members and the solutions and services they provide are not built such as other industries; they are rarely tangible, physical, or in any way restricted by physical borders.

Currently, enterprises themselves are not required to carry out responsibilities that involve security monitoring and security audits of their operational technology solutions, leaving security vulnerabilities within European critical infrastructure enterprises. A recent study found that over 13,000 vulnerabilities were found (in EU and US based critical infrastructure enterprises) in commonly used operational technologies solutions.[68] This issue, leaving connected enterprises without the ultimate responsibility of taking care of their own IT and OT infrastructure, networks, and the needed protective measures, puts the continuity and operative reliability at risk of being halted by an offensive attack conducted through a vulnerability. The connected enterprises that are actors of European Critical Infrastructure are also creating an unnecessary risk through their own vulnerabilities and heightened risk of falling victim, leaving Europe and Europeans open to attacks. Energy, foodstuff, transportation, healthcare, and a number of critical infrastructure sectors are reportedly heavily targeted by cybercrime.[69]

Critical infrastructure enterprises are identified as crucial to the economic and human safety of the Member States. The introduced legislation banking and financial industries is a clear trickle-down effect that banking and financial services as well as maritime enterprises and those that work with the sector providers have needed to take as precautionary and preventive

[67] European Commission 2020d
[68] Anton et.al. (2021)
[69] KPMG Harvey Nash 2019 CIO Survey, Table 1

measures, as outlined in directive 2016/1148. Industry differences are apparent: industries with stricter regulation such as financial sector are less likely to suffer security breaches; in several management consultancies studies and assessments ICT security cybersecurity and network security executives have listed the security incidents and malice attacks they might have experienced. In the 2019 KPMG Harvey Nash global CIO Survey, roughly a third of CIO's have reported cyber-attacks. In Table 1 the percentages of CISOs reporting attacks are displayed as a reference for a sector specific comparative analysis.[70]

[70] KPMG Harvey Nash 2019 CIO Survey, Table 1

Sector	Major cyber-attacks experienced and reported by CIO's within each sector, in %, 2017-2019
Telecommunications	44
Transportation / Logistics	40
Leisure	39
Broadcast / Media	38
Construction	38
Education	37
Manufacturing	35
Pharmaceuticals	35
Government	34
Healthcare	33
Retail / Consumer goods	33
Global average	32
Oil & Gas	31
Power & Utilities	31
Financial Services	30
Business / Professional services	27
Technology	26
Charity / Nonprofit	21
Average	34

Table 1: sector specific responses on cyber related incidents: "KPMG Harvey Nash global CIO Survey, roughly a third of CIO's experienced cyber-attacks" shows alarming percentage of most major industries impacted.

As laid out in Chapter V of the NIS Directive, the current European cyber legislation does not cover one of the most vulnerable types of adopted enterprise solutions: the operational technologies. The often niche and single purpose serving solutions run the core operations and

services the organization or enterprise provides. Even though OT carries an undisputed relevance to the enterprises they are a part of, these systems are not currently covered by European cybersecurity legislation. The reason why they are out scoped is that often the developing and managing IT providers are very small by the size of their annual revenue.

The new legislation introduced in this thesis prevents service and solution providers from continuing the commonplace practice of removing cybersecurity related management responsibilities by mandating the enterprise itself as the ultimate party responsible of the solutions and services that they have chosen to run in their technology stack. This thesis continues by suggesting a framework that should be the basis of the requirements mandated by EU law. Cyber certificates and related cyber audits were mostly voluntary in nature, unless discussing organizations that directly are in business with government contracts or specialty sectors, listed on the EU Commission's website, financial sector being an example. Though there are some mandatory certificates for specific actors, there are plenty of enterprises that are members of the critical infrastructure, but fall outside of the are designed to help organizations follow a proven and well-designed framework that, in essence takes the burden of designing and maintaining from solely the CIO's office, and provides assistance in designing, and then checking against benchmarked and ever developing set of criteria.[71]

[71] Iaiani et.al. (2021)

8 Legal maneuvering that leads to diminished responsibilities

Traditionally private data centers, servers etc. are the company's own responsibility, or a ready-made solution provided by a large organization. Public cloud and large IT service providers have changed how IT risk models work significantly. The risk models and responsibilities are increasingly dynamic, subject to constant changes, and have become shared between the enterprise, and its IT & OT providers. With Infrastructure as a service, the cloud provider manages virtual servers, operating systems, and the data you bring on the platform. It is important to understand whether you're consuming IaaS, PaaS or SaaS. Responsibilities that change depending on the adoption model and their risk models according to how you're consuming, and who is providing which part of a fragmented service: maintenance, hosting, connections and networks, application operations, cybersecurity, access management, service desk etc. The different providers and the connected enterprise (the client) are always in a fluid and blurry compliance limbo. It is near impossible to directly point out the responsible parties with current legislation, and a new framework with a centric responsible party needs to be appointed.

As an example, responsibilities of the cloud provider could include: The cloud provider is responsible of managing the security of the platform so that it is compliant, secured network, secured managing runtime, isolation and containers, so that the client has its own space within the public cloud platform. While responsibilities of clients could include: Platform as a service (PaaS) in a nutshell; you're building applications, migrating applications to the cloud, and running them in the cloud. You're responsible for securing the applications you build, the workloads, and the data. Additionally, a couple of other third-party providers could have contracts for monitoring IAM access management of internal and external users, application operations of a third of critical operational technologies, and as well as the SOC security command center operations.

Without legally mandating the connected enterprise to take legal responsibility as the orchestrator, it is near impossible to draw clear lines for securing our critical infrastructure in a systematic way. In essence, responsibilities that change depending on the adoption model and their risk models according to how you're consuming.

Small IT operators, service and solution provers are not in the scope of the new Cybersecurity Act and NIS2 amendments. In practice that means, that our critical infrastructure's connected enterprises that use operational technology solutions provided by niche providers have no legal mandate to be protected sufficiently. By making enterprises responsible for OT SEC, (or make them purchase it as a service), we bring clarity for what responsibilities and what regulatory measures should be taken to introduce EU-wide improvements to critical infrastructure enterprises' cybersecurity.

Future scenario: The European Union introduces new legislation that proceeds to strengthen our enterprises cybersecurity across the middle, back, and IT office, without excluding the small operators from the law.

Currently Large IT superpowers with off-the-shelf software act as partners to enterprises. The large providers Amazon uses enterprises data as their right - the price of cheap software is attractive, instead of the costs of internal IT developing solutions that do not need much tailoring themselves. The sheer mass of large IT providers makes it possible for them to uphold very high cybersecurity standards and protocols and have immediate response in the event of an unlikely cyber related event would occur at a client IT/OT environment.

Small providers on the other hand often provide the most production or service critical operational technologies, the ones that are extremely tailored or coded from scratch to serve a detailed and specific purpose. These are extremely vulnerable for attacks, as no one takes real responsibility of the developed technologies. The small providers are in a low margin business; they do not have the resources and the manpower, and enterprises at this time are not required by law to act on OT security

9 The significance of the proposed new framework for operational technologies

The most important operational technologies solutions are located close to the core operations of the enterprise, for example the solutions running on the factory floors, in energy pipelines, in energy distribution, inside nuclear plants. They are close to all of other critical infrastructure enterprises core operations and manufacturing are highly specific, made to serve a specific purpose and often developed by a small internal team or a small IT provider that is specified to serving very specific clientele and deliver tightly narrowed types of software.

The burden for a small vendors to take the financial responsibility of the continuous service, monitoring, and audits, would be too much, which is why Article 16 of the NIS directive rightly out scopes, as this thesis agrees that mandatory certificates and heavy audits would be very likely an overkill, causing a small-margin small OT provider to have a hard time to stay profitable. Instead of scaling the same design principles that fit the large DSPs and OES's, in essence the legal design used for drafting NIS2 that regulates the large providers, protective measures and the attached financial burden should be required from the enterprise that runs them in their IT/OT environment. Regardless of it being a managed service or a shared responsibility software where both the software provider and the company share managed services, the burden of processes, documentation, and audits should be on the enterprise's responsibility.

This means, that the most important pieces of software within enterprises are software that is completely excluded by current European Cybersecurity Act's and Directive's scope, as the current EU cybersecurity legislation excludes both small service and solution vendors and the client enterprises from carrying the responsibility by its consideration of the financial burden being too great for small vendors and by failing to consider the client enterprise the final responsible party of their own IT/OT environments and connected networks. Others have also noted the inadequacy and shortfall of the proposed revised directive (NIS2) Directive, and that

European cybersecurity legislation still fails consider some of the most vulnerable parts of enterprise IT in its' scope.[72]

[72] Christou (2018)

10 Proposing a new mandatory framework

10.1 The framework

Connected enterprises are as secure as their weakest point. Often hacks in the critical infrastructure happen through exploited operational technologies weaknesses. That is why it is vital that both executive and operational leaders of the organization are keen to audit their own security policies, practices, and systems. Security assessments for OT compliance measure systems controls against the legal requirements, and that OT systems create the appropriate technical and organization measures to ensure a level of security appropriate to each risk.

Subjecting the organization to regular testing with honest third-party assessments and evaluations that are shared top-down leads to both technical and procedural security that upholds the legislative requirements, as well as help birth an ethically sound culture of care for privacy and secure data handling within the organization.

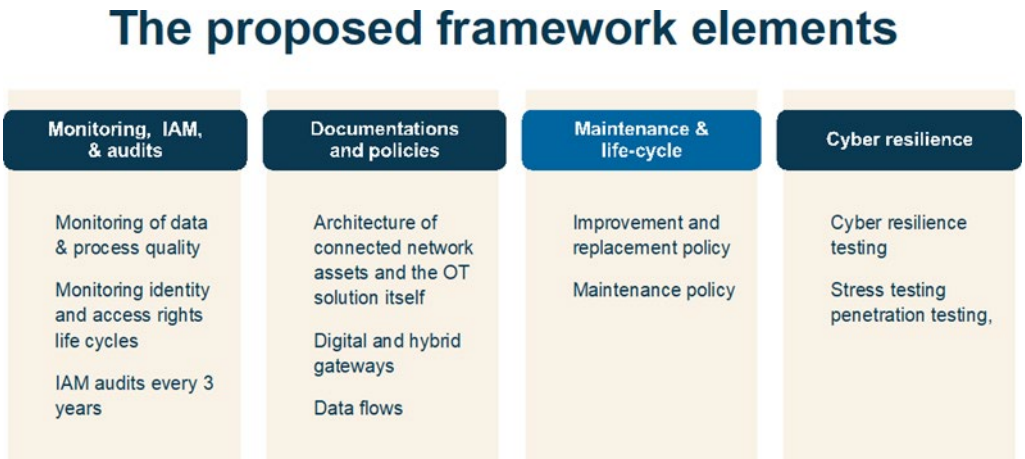

Figure 1: The proposed framework elements.

Please see figure 1 for an overview of the framework. The framework acts as a top-level guide for creating documentation, policies, and audits for enterprise IT and OT assets not provided or managed by a certified provider. A clear example of the division would be a

public cloud service provider like Google Cloud, or a small startup OT software made for managing a paper mills output and managed by enterprise's own IT professionals.

The framework includes process documentation, mandatory monitoring, policies for maintenance and life-cycle management, policies and audits for identity and access management policies, and OT architecture documentation of solution, interfaces, digital and hybrid gateway and connected networks levels. Data flows across the enterprise stack and attached systems and networks should be documented as well to whichever part they are related to the OT solution.

The proposed framework has factored in risks and proposes preventive process documentation and mandatory mapping of OT architecture as ways to mitigate the risks significancy. The processes and documentation should help identify the current OT landscape to design specific protection measures to prevent a cyber-attack against OT systems commensurate to the business risk. Deploying specific protection measures to prevent a cyber-attack against OT systems, establishing mechanisms for identifying attacks, undertaking appropriate action in response to confirmed security incidents against OT systems is crucial.

The leaps in development of interconnected networks, systems, and technologies has increasingly sped up. Data and information are being harvested, transferred, stored, combined, analyzed, and utilized in unprecedented ways across complex interconnected networks, IT/OT environments, and systems from factory floors to business software solutions.

11 Understanding the findings

11.1 Further analysis of the research questions

This thesis presents three research questions to bring structure, and to ease the legal and technical analysis of the current EU-wide cybersecurity legislation and ENISA's role in European cybersecurity, prior to combining the findings of the combined legal and technical analysis.

1. Does the current European Directive of Network and Information Security (NIS), and the proposed revised directive (NIS2) and the European Cybersecurity Act together, with the official guidelines released by ENISA, form a sufficient layer of mandated cybersecurity protection for connected enterprises and digital infrastructure?

With the modern enterprise IT/OT environments that operational technologies exist in, the current EU-wide NIS Directive, the proposed revised directive (NIS2), and the Cybersecurity Act, together with ENISA are not sufficient in protecting the entirety of the IT/OT environment assets, especially regarding the operational technologies. New EU legislation is highly suggested for operational technologies, as their nature has changed from being isolated solutions, to being connected to the Internet and the surrounding enterprises connected networks and IT infrastructure.

Operational technologies solutions were designed to serve a narrow purpose, often directly related to enterprise core business operations, the manufacturing of a product or a service. They were standalone or at least isolated solutions, with localized control. They were designed to be reliable and safe to operate, rather than being secure.

With continuously increasing connectivity, OT systems are no longer isolated; they are a part of the connected enterprise IT environment and networks with information flowing to and from the previously stand-alone solutions. Commercial off the shelf OT solutions are just as common as co-developed or internally (within the enterprise) developed solutions. Once integrated, the monitoring and support services may be internally managed by the IT department, or outsourced fully or partially to one or more vendors, which may be other than

the party that initially participated in the development of the system.

The proposed revised NIS2 Directive, the EU-wide cybersecurity law, excludes small and medium digital service providers (DSPs) outside of the scope of it, which is the core reason why this thesis was written. "*To avoid imposing a disproportionate financial and administrative burden on operators of essential services and digital service providers, the requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. In the case of digital service providers, those requirements should not apply to micro- and small enterprises*."[73] Understandably, finding the sweet spot in balancing between imposing security related financial responsibilities and encouraging adoption of solutions and speeding digitalization is anything but straightforward. Regardless, this thesis wants to bring light to the current vulnerabilities that exists in connected enterprises, especially regarding operational technologies, as well as the issues in how current EU-wide cybersecurity legislation is built.

Connected operational and process systems, some that have been developed for a specific task and that have been in production for decades, are a part of developing digital environment, with an ever-connected nature. With enterprise technology stack being increasingly connected, the operational technologies solutions meant to work in isolation, are being connected to a wider infrastructure and multitude of business systems, production solutions, and core enterprise operations solutions. As Caldwell writes (2018) that "*the integration of systems that have traditionally run machinery as standalone, closed-in operations with the Internet has created both an opportunity and a challenge*."[74]

2. How can small OT solution vendors and service providers be made responsible for the cybersecurity of their portfolio offerings without over-bearing their business by the massive size discrepancy of their client enterprises? Many vendors serve clients that are more than hundredfold larger than they are.

It is impossible to mandate the small providers of enterprise operational technologies to carry the financial burden of managing services or the continuity of solutions within connected

[73] Directive (EU) 2016/1148 (53)
[74] Caldwell (2018)

enterprise IT/OT environments, which is why the current legislation is capped to the large providers of infrastructure, platforms, and software as a service providers. With the most critical layer of digitization, the operational technologies that run European critical infrastructure is therefore out scoped by current European cybersecurity legislation; "*In the case of digital service providers, those requirements should not apply to micro- and small enterprises*".[75]

The new legislation introduced in this thesis prevents service and solution providers from continuing the commonplace practice of removing cyber security related management responsibilities of OT solutions, by mandating the enterprise itself as the ultimate party responsible of the solutions and services that they have chosen to run in their technology stack.

The proposed revised (NIS2) Directive, considerably the most potential legislation to be used to protect the whole of an enterprise IT/OT environment, falls short of its intention to do so. The EU-wide cybersecurity legislation out scopes operational technologies vendors by size as operational technologies solution and service providers are often small and cater only for a very specific purpose solutions, which makes them free of the burden of from large IT providers. The current legislation is capped to the large providers of infrastructure, platforms, and digital service providers (DSP).

Operational technologies that run European critical infrastructure is scoped outside of the Cybersecurity Act, The NIS Directive, and the proposed revised NIS2 Directive. The current European cyber legislation does not cover arguably the most vulnerable type of adopted enterprise solutions: the operational technologies. The reason why they are out scoped is that often the developing and managing OT/IT providers are very small in headcount and annual revenue due to the very specific purpose solutions they cater to a very limited number of clients.

IT industry has mastered managing distributed service offerings and risk to a point where only the largest providers in the global market has to take full responsibility of their solutions and services. This phenomenon leaves a great part of enterprise IT stack poorly protected in the EU. The same phenomenon is a problem the construction sector is facing. In construction, house building projects are contractually negotiated by subcontracts, which lifts the overall

[75] Directive (EU) 2016/1148

responsibility off of the builder: as no one can point to any given dynamic construction project's group builders and single out the main contractor out of a group of subcontractors. The issue is at core the same in both industries: larger project portfolios volumes of work are disguised behind subcontracts. The IT industry's service and solution providers may also have diverse portfolios that separates the standard solution and managed services into many subcategories that they sell either separately or as a bundled offer. Contractually diversifying their contracts and offerings makes them subcontractors, and in that way able to partially or in full mitigate the possibility of having to take responsibility of preventing cybersecurity related incidents.

3. Why does such a legally mandated framework for operational technologies matter?

European Union needs to design its own certification framework that supports the Single Digital Market strategy. A legally mandated framework would strengthen overall European cybersecurity and digital infrastructure resilience against attacks.

11.2 Associated risks and risk bearing

Determining large tech providers' responsibilities may be difficult as legislation is barely covering them, and a shared service model has blurry lines between different stakeholders and the degree of which they are responsible of product and associated risks. The proposed new legislation introduces that like major IT providers offering as-a-Service proprietary technologies and/or their support are responsible for maintaining legally required processes and documentation for the provided Iaas, PaaS, and SaaS -services, enterprises are responsible for the OT provided by small service and solution providers.[76]

Enterprises' digital infrastructure is becoming increasingly independent of hardware, making processing, storage, and network functions virtualized and outsourced, with shared responsibility or fully outsourced responsibility. Some commonly known examples are

[76] Marston et al. (2011)

Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) technologies.[77]

In the future Cyber as a Service (CaaS) will develop into a significant service within the European Union. One of the drivers that will impact the development of centralized and outsourced cybersecurity services is law. Especially if the legal instruments are similar to the ones proposed in this thesis' legal framework.

As-a-service technologies regulation-wise cannot be dealt with on a case by case basis but needs laws with a holistic approach. The EU does not need to completely substitute or change the existing legal tools; however it should complete it with laws to realistically regulate the IT/OT environments where cybercrimes take place. The most prominent field of this kind nowadays is probably the cloud.[78]

11.3 Making enterprises take on responsibility for the small vendor solution security within their connected IT/OT environments

Digital services providers like Microsoft, Amazon, and Google have developed an all-around portfolio of offerings that combine virtualized and outsourced hosting of IT infrastructure, IT platforms, and enterprise IT software assets of the front-, middle, and the back office. New responsibilities introduced in the risk models and responsibilities as management of IT operations and assets are partially shared between the public cloud provider Operators of Essential Services (OES) and Digital Service Providers (DSP) are required to adopt risk management practices, and without delay notify incidents to national authorities.[79]

The Article 16 of the NIS Directive outlines that the directive does not apply directly to organizations, which indicates that its purpose is not to impact by describing enterprise's minimum mandatory security measures or minimum mandatory zero-day incident response procedures designed to limit offensive attacks and their impact. The NIS Directive rather is a

[77] Marston et al. (2011)
[78] Kontargyris (2018), p. 73-74
[79] Marston et al. (2011)

guide to Member States with aim on making national legislative bodies ensure that legislation is drafted that meet the mentioned minimum requirements.[80]

the proposed revised NIS2 will strengthen the security requirements with incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption. Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.[81]

Integrations and network assets that make it possible to outsource IT services can be managed by enterprises, large IT solution. and service providers, or third parties with a part of the maintenance or management responsibility of an IT solution that is being used in any given enterprise. Responsibilities of integrations, network assets, solutions, life cycle management, cybersecurity, identity and access management (IAM) are shared currently between solution providers, the same or perhaps several a different managed service provider, and the enterprises themselves. They can be novel code or altered solutions. Currently a major issue is that almost all enterprises use solutions that no one knows to detail, that are not governed with appropriate lifecycle and maintenance policies.

Recommended risk-management measures for enterprises to follow include taking full ownership of the overall responsibility of the operational technologies is vital, for one party to have the big picture of what is implemented into their IT/OT environment. These environments are extremely complex, with plentiful of integrated solutions and remotely operated solutions or networks. This means, that no matter what size of vendors are small or the responsibility is contractually shared and therefore hard to pinpoint to any vendor, or when there is ambiguity that partially or fully outsourced solutions bring with them, the enterprise must be the final party responsible for their own digital infrastructure. If the enterprise itself does not want to take full responsibility of overseeing their digital infrastructure, they should be allowed to outsource that to one service provider that would act as a shadow CIO and take full responsibility of the suggested tasks. Risk management documentation and written processes are extremely important in ensuring preventive measures and reactive measures are easily made in time. Information technologies and operational technologies solutions, network architecture,

[80] NIS Directive, Article 16, (53 and 57)
[81] European Commission 2021a

master data flows, identity and access management, as well as digital and hybrid gateways need to be documented.

Systematic protection of enterprise's digital infrastructure and networks are critical to human and economic safety. The European cybersecurity legislation lacks flexible yet comprehensive framework that regulates and mandates critical infrastructure enterprises to protect their operational technologies stack, in connected enterprises lacks preventive and protective actions and protection in the digital era.[82]

[82] Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience

12 Suggestions for EU legislators: a quick-to-read brief

12.1 Risk-management measures

Enterprises need to carry the overall responsibility for operational technologies implemented into their IT stack that are:

- Delivered by small IT solution and service providers
- Excluded from other cybersecurity legislation (small size excludes them from current legislation)

12.2 Holding the enterprise responsible

The enterprise itself needs to have final responsibility or appoint a responsible party for overseeing the complex technology stack and its operations:

- When the current cybersecurity legislation does not apply (solution and service providers are too small, or the responsibility is shared and therefore non-existent)
- When partially or fully outsourced to several service providers, (i.e. the solution/application, application operations, monitoring, network assets, and access management are provided by different vendors)

12.3 Risk management documentation

- Identity and access management in place
- Digital and hybrid gateways of OT documented across the connected enterprise, to form a clear picture of enterprise security operations
- IT, OT and network architecture pictured, and data flows documented

12.4 Effective use and documentation of encryption for all OT not covered by a service or solution provider that falls under current cybersecurity legislation

- Off-the-box solutions
- Co-developed solutions
- Self-developed solutions
- Solutions with partial operations or hosting by a provider
- Solutions with managed shared services contracts have indicated responsibility transferred over to the service provider (this shields the intended purpose of this proposed legislation against enterprise legal departments from continuing the shared services business, and the industry's standard act of all parties avoiding taking responsibility by sharing services among different providers)

12.5 Maintenance and life cycle management

- Documentation and processes in place always

12.6 Incident prevention and response processes in place

- Mandatory annual reporting of cybersecurity assessment to national authorities
- Take responsibility of patching based on findings
- Notifying authorities of significant incidents
- Vulnerability handling and disclosure, processes
- Encryption in use according to processes across the enterprise IT/OT environment assets
- Authorities can audit or assign third parties to audit OT systems used in critical industries enterprise

13 Conclusions

This thesis has analyzed the current European-wide cybersecurity legislations. The main questions of this thesis were whether a sufficient layer of mandated cybersecurity protection for connected enterprises and digital infrastructure exists, how small operational technologies solution vendors and digital service providers could be required to take responsibility for the cybersecurity of their solutions, and why does the proposed legally required framework for operational technologies matter.

To address the research questions of the thesis, a legal dogmatic method, also known as legal doctrine, is applied. Dogmatic research has two dimensions or purposes: interpreting the content of existing legislation and systemizing the legislation. To tackle the first goal of the dogmatic research method, the roles of the current EU cybersecurity laws; the Network and Information Security Directive (NIS Directive), the proposed revised directive (NIS2) as well as the European Cybersecurity Act that mandates ENISA to propose future European certifications for our Internal Market are analyzed. Based on this analysis, it is easy to conclude that a gap exists in current EU-wide legislation. The core issue is that sufficient cybersecurity actions are not required from micro- and small vendors, which directly leads to the most vulnerable, operational technologies being excluded from the scope of current EU cybersecurity legislation. To tackle the second goal of the dogmatic research method (systemizing the legislation), the framework is proposed.

The proposed framework includes requirements for process and life-cycle management, connectivity and solution architecture documentation, and up-to-date policies for identity-, access management, and information security, with regular audits and pen testing. The proposed framework has factored in risks and proposes preventive action to mitigate the risks.

Fundamentally, instead of imposing disproportionate financial and administrative burden on small vendors to bridge the existing gap, the purchasing enterprises should take on or outsource the final responsibility of securing and monitoring their digital infrastructure, connected networks, and integrated solutions.

The key point is that the European Union needs to design its own, modern certification framework that supports the successful implementation of the Single Digital Market Strategy and ENISA's goal of strengthening trust in the connected economy, boosted resilience of the Union's infrastructure and services, to keep our society cybersecure. A legally required framework would strengthen overall European cybersecurity and digital infrastructure resilience against attacks.

After the introduction of the Cybersecurity Act in 2019, ENISA has had a stronger mandate to begin working on future European cybersecurity certification schemes. A draft document EUCC V1.1.1., which is a candidate cybersecurity certification scheme, is circling on the tables of industry professionals for commentary. The document is at this time a very rough, preparatory legal text, and not even considered an official publication. It will be interesting to see how the cybersecurity certification scheme will take form, and whether the final version manages to bridge the existing gap between current European cybersecurity legislation and enterprise cybersecurity as proposed in this thesis.