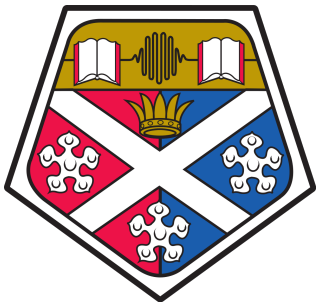


Mutual Influences of Cybersecurity and Law

Kaspar Rosager Ludvigsen

A thesis presented for the degree of

Doctor of Philosophy

Department of Computer and Information Sciences

University of Strathclyde

Declaration

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Signed: Date: 11th December 2024

Acknowledgements

I would like to first thank my supervisors for their guidance and collaboration. In alphabetical order: Angela Daly, Shishir Nagaraja, Crawford Revie and Birgit Schippers. It was a joy to work with you all, and I look forward to future collaborations.

I thank Vassilis Galanos for some of the core inspiration for the reasoning behind this thesis. I equally thank Elisabetta Biasin and Erik Kamenjašević for their collaboration and support. A special thanks should also be given to Marco Almada for his encouragement and inspiration.

I thoroughly thank my parents, Paw and Sanne, my brother Aske, my ex-wife Anouchka, Rocky the cat, Molly the Golden Retriever, Oskar the dog, Miko the cat and Leia the cat for the emotional and practical support which was crucial for the success of the project.

I also want to also thank my examiners for their extensive and constructive comments!

Finally, I thank all my colleagues, peers from other universities, senior academics, my students, and neighbours who helped me in various ways. It was all very appreciated!

And an extra thank you, to *you, the reader*! You are an important reason why I would go through this all over again, if I had to.

Abstract

The use of computers at every level and place in society comes with costs in terms of cybersecurity. The positive effects of the current usage of digital devices and software are ease, speed, and exponentially reducing costs. The disadvantages are adversaries being able to attack individuals, corporations, and states at any time and at any point . The use of software and hardware has become the norm, and they are embedded and used everywhere in society. The law must adapt to understand this new digital reality. This thesis tackles this problem in three different themes.

For legislation to work, it must cover the necessary legal subjects. This is a problem facing Medical Device Regulation in the European Union (EU) and this thesis suggests expanding the notion of intention. While it may prove more costly for the authorities and manufacturers, it will benefit patients in the form of increased security, and therefore safety. The thesis also clearly shows how cybersecurity should be understood within the context of the Regulation. A unique cybersecurity-based taxonomy for attacks on surgical robots is included, also used in the case law analysis provided, consisting of a small analysis of Danish law and procedural considerations regarding reimbursement cases involving cyberattacks in court. The thesis finds that reimbursement involving cyberattacks should be possible, demonstrating that flexibility within the law is required for it to function within a technologically changing society.

New surveillance technologies bring new Human Rights and technology-based threats. In the case of Client-side Scanning, the focus is on what happens when these technologies break, leak, or are manipulated. First, a new definition of Client-side Scanning is created, followed by a cybersecurity analysis of the term. The thesis then shows how these systems can be a risk, but also how other Client-side Scanning systems may be considered in the future within the framework of the European Human Rights Convention. While privacy is always at risk regarding surveillance systems, the thesis notes that things like admissibility of evidence and incrimination may also be difficult issues to handle within the Convention, and that states should carefully legislate for the usage of the systems to ensure that they do not violate the Convention.

Resilience is a central tool to enable robust cybersecurity, both in a legal and technical sense. The upcoming legislation in the EU, the Cyber Resilience Act, is an important step towards enforcing resilience in practice on all digital systems. Together with existing and upcoming regulation, it paves the way for a higher level of security and compliance, even if it is limited by its reach as product legislation. The thesis analyses the Act in the context of supply chain cybersecurity and discusses two cases of supply chain attacks and the implementation of NIS 1 in three jurisdictions. A picture emerges of a significant gap between national cybersecurity and internationally–founded supply chain security. While this raises concern and criticism, the Act does offer some solutions to the clear issues presented by Supply Chain Security.

Contents

List of Figures

Published Work

Below is a list of publications which were written alongside the thesis.

Conference Proceedings

- Ludvigsen, Nagaraja, Daly, "Preventing or Mitigating Adversarial Supply Chain Attacks: a legal analysis", ACM CCS SCORED '22, 2022, https://doi.org/10.1145/3560835.3564552.

Journal Articles

- Ludvigsen, Nagaraja, Daly, "When Is Software a Medical Device? Understanding and Determining the "Intention" and Requirements for Software as a Medical Device in European Union Law", *European Journal of Risk Regulation*, September 2021, https://doi.org/10.1017/err.2021.45.

- Ludvigsen, Nagaraja and Daly, "Dissecting liabilities in adversarial surgical robot failures: A national (Danish) and EU law perspective", *Computer Law and Security Review*, Volume 44, April 2022, https://doi.org/10.1016/j.clsr.2022.105656.

- Ludvigsen, "The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions", *Law, Technology and*

Humans, Volume 5, Issue 2, November 2023, https://lthj.qut.edu.au/article/view/3080.

Preprints

- Ludvigsen, Nagaraja, Daly, "YASM: Yet Another Surveillance Mechanism", May 2022, https://arxiv.org/abs/2205.14601.
- Ludvigsen, Nagaraja, "The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity Resilience Act", May 2022, http://arxiv.org/abs/2205.13196.
- Ludvigsen, Nagaraja, Daly, "The Dangers of Computational Law and Cybersecurity; Perspectives from Engineering and the AI Act", July 2022, http://arxiv.org/abs/2207.00295.

Other publications

- Lindstadt, Ludvigsen, "When is the Processing of Data from Medical Implants Lawful? The Legal Grounds for Processing Health-Related Personal Data from ICT Implantable Medical Devices for Treatment Purposes Under EU Data Protection Law", Medical Law Review, 2022, https://doi.org/10.1093/medlaw/fwac038.
- Biasin, Kamenjašević, Ludvigsen, "Cybersecurity of AI medical devices: risks, legislation, and challenges" in *Research Handbook on Health, AI and the Law* (Edward Elgar 2024).

1 | Introduction

Any digital system is vulnerable to cyberattacks and must deploy defences; this makes cybersecurity as a sub-discipline under computer science more important than ever. Due to the increased use of digital devices across every aspect of society, all parts of our lives are now more vulnerable from cameras, banks, smartphones, medical devices, and critical infrastructure. Good intentions from manufacturers, while positive, are not enough in this scenario, hence societal tools such as laws and regulations must be employed to guarantee safety and security for everyone.

This thesis sets out to explore how law and cybersecurity interact, asking the questions of "how can this legal concept be understood in cybersecurity," and conversely, "how can these cybersecurity considerations be understood in law". These two questions will be asked at the end of each chapter and answered accordingly, and the conclusion of this thesis will offer broader answers to them. The thesis consists of three distinct cases, each explored in their own chapters, and each offering widely different perspectives on both the law and the cybersecurity aspects chosen. These three case studies also provide diverging answers to the two questions and to the exploration as such. The first zooms in on medical devices, the second on client-side scanning, and the third is about supply chain cybersecurity and resilience.

The thesis acknowledges the legal environment in which cybersecurity ex-

ists, while also understanding the reality of deployment and practical considerations that apply equally.

Advancing the knowledge necessary for the research on understanding the impact of law on cybersecurity, and cybersecurity on law, is also a contribution. While primarily focused on EU law, the analysis done in this thesis will be relevant to many other legal systems. And while law plays the largest role, theoretical understandings of security are also necessary if we are to fully comprehend how this functions.[1]

We reap the benefits of at least fifty years of solid safety engineering, risk management, and security engineering experiences, and we can make our systems and lives safer and more secure through these. The argument against improving safety and security, that it makes everything slower and more expensive, has been the same since the inception of encryption.[2] This was not empirically founded back then and is not supported academically currently outside of increased costs.[3]

One thing is for certain, and that is the ever-increasing complexity of building safe and secure systems. The more elements that are added to something, the more complicated it will be to manage, and this is best illustrated with medical devices. Syringes, surgical meshes,[4] and scalpels are regulated by the same legislation as surgical robots, pacemakers, and insulin pumps. The latter three examples must both consider cybersecurity and safety at the same time and do not have many years of incidents and stan-

[1]This is also to fulfil the interdisciplinary aspect, see Jaako Husa, Comparative Law and Interdisciplinarity, "Law &" (An Encyclopedia of Interdisciplinary Studies, Hong Kong University 2024) 3.

[2]Auguste Kerckhoffs, "La cryptographie militaire" (1883) IX Journal des sciences militaires 5 ⟨http://www.petitcolas.net/fabien/kerckhoffs/⟩.

[3]Ross Anderson, *Security engineering: a guide to building dependable distributed systems* (John Wiley & Sons 2020). And these may be recuperated from the decrease in safety and security incidents.

[4]For specific issues with these, see The Independent Medicines & Medical Devices Safety Review, *First Do No Harm, The report of the Independent Medicines and Medical Devices Safety Review* (techspace rep, 2020).

dards to guarantee a minimal level of safety.[5] This calls for legislative solutions and focus, meaning that just in this case alone, tight cybersecurity regulation is warranted.

The analysis is carried out through a multi- or interdisciplinary methodological lens that marries law, cybersecurity, and engineering, but this varies from chapter to chapter; some will be interdisciplinary, while others will be multidisciplinary.[6] This can be seen as a contribution of the thesis. As mentioned above, the main contributions of the thesis are expressed through various themes in each chapter, which provide an overview of the interaction between cybersecurity and law. Another contribution comes in the form of posing future research questions in each of these chapters.

Technology and law are intimately connected. This statement has genuine merit as any law, legal system, or enforcement of rules throughout the law's existence has been expressed in the technology of the time.[7] Methods of corporal punishments, currency, and structure of armies are all historical, yet there are contemporary examples of how the use of technology matters. The choice of technology may also influence what the law should be or does. While law can exist without tangible tools,[8] it usually requires the bare minimum of physical media to preserve, maintain, and execute it as humans have much more limited lifespans than stones, papyrus, and paper.

---

[5] On the contrary, see ibid.

[6] For more, see the overview in Chapter 2.

[7] See, Howard Mumford Jones, "Ideas, History, Technology" (1959) 1(1) Technology and Culture 20 ⟨https://www.jstor.org/stable/3100784?origin=crossref⟩; Yehezkel Dror, "Law and social change" (1959) 33(4) Tulane Law Review 787; Quincy Wright, "Inferences of Science and Technology for International Law" (1955) 4(2) Journal of Public Law 358.

[8] Examples of this include oral contractual agreements, later enforceable in court, and civic trading and conflict solution. Past systems may have employed memorisation systems that could enable full oral law, but the scale and ease which physical media bring far outweigh the benefits of it. We see parallels to the digital development of legal systems currently, Rikke Frank Jørgensen, "Data and rights in the digital welfare state: the case of Denmark" (2021) 0(0) Information Communication and Society 1 (Publisher: Taylor & Francis) ⟨https://doi.org/10.1080/1369118X.2021.1934069⟩.

Law, as a term, not only exists in the medium where it exerts its influence. The law and the legal system can be seen as separate entities, in which the law lives its own life even though it may be affected by the types of technology available to it. An examination of the changes in the ways in which criminal cases have typically been handled over the past few decades illustrates this. Principles and many rules will not be changed in order to negotiate, understand, and contest contracts. Despite this, courts changing to fully digitized systems will have a concrete effect on how fast pre-trial procedures are run. Sharing documents with the opponent, which one advocate thinks will convince the judge, becomes instantaneous and changes both the speed and potentially causes unforeseen effects compared to the past paper-only culture.[9] This change in technology includes cybersecurity, in the form of the platform which the advocates and judges use, and all their respective use of emails and smartphones as individuals. This creates a multitude of security entry points and, as a result, the perspective becomes entrenched. This will be explored in this specifically thesis.

Law being heavily affected by and incorporated into digital technology is a recent idea, expressed in concepts such as code as law.[10] Further effects came through connectivity in the form of ease of communication, with everything from Morse code to modern peer-to-peer networks, and the infrastructure of the internet. Looking further back, even transistor development and means to express logic outside of ourselves and execute

[9]There are no empirical or legal studies on this yet, but it has been in discussed by, e.g., Jan Oster, "Code is code and law is law—the law of digitalization and the digitalization of law" (2021) 29(2) International Journal of Law and Information Technology 101 ⟨https://academic.oup.com/ijlit/article/29/2/101/6313392⟩; Mireille Hildebrandt, "Code-driven Law: Freezing the Future and Scaling the Past" in Simon Deakin and Christopher Markou (eds), *Is Law Computable?: Critical Perspectives on Law and Artificial Intelligence* (Hart Publishing 2020) ⟨http://www.bloomsburycollections.com/book/is-law-computable-critical-perspectives-on-law-and-artificial-intelligence⟩; Jon Christian Fløysvik Nordrum and Ingunn Ikdahl, "En vidunderlig ny velferdsstat? Rettsstaten møter den digitale velferdsforvaltningen" no (2022) 25(3) Tidsskrift for velferdsforskning.

[10]Lawrence Lessig, *Code and other laws of cyberspace* (OCLC: ocm42860053, Basic Books 1999).

actions or calculations have actively affected law. We may have been able to express logic (including legal arguments) on the abacus and blackboards before digital technology, but law had to be deployed through human beings. Now, expressing the logic through systems which are protected and enabled by cybersecurity, leads to situations where it can also be attacked directly by its adversaries. One is still able to affect the individuals expressing the logic of law in practice, but the ability to attack digital legal systems from anywhere in the world, at any time, is an escalation beyond the risks of the past and brings the conundrum to a much greater scale.

1.1 Structure

Chapter 2 reveals the necessary background to understand the rest of the thesis in law and cybersecurity, and the methods used. It does not attempt to give the full overview, as each chapter has its own background included. Secondly, the chapter includes explanations of doctrinal and comparative methods for law, and theoretical computer science, together with theoretical engineering methods for cybersecurity. Comments on the advantages and disadvantages of multi- and interdisciplinary methodology are also included. Finally, an overview of the methods of the subsequent chapters that follow is given.

Chapter 3 analyses legislation and understandings uniquely held by the medical device community, which is inherently interdisciplinary[11] and at the same time part of the critical infrastructure of any country,[12] making it an example of cybersecurity regulation directly affecting the security and

[11]For medical devices to be designed, deployed, and used, lawyers, engineers, and medical practitioners are needed.

[12]Medical Devices directly (idiosyncratic surgical robots) or indirectly become part of the critical infrastructure of a country. This is due to them being essential for the functioning of any type of healthcare system, which is considered critical infrastructure.

safety of individuals in a physical setting. The primary source of medical device legislation in the EU, the Medical Device Regulation,[13] is explored in detail. Firstly, the thesis focuses on what constitutes a medical device specifically with regards to software and hardware, and secondly, on how liability, rights, and obligations function, and how remedies to the issues which adversarial attacks on surgical robots bring can be conceived and solved in a single national legal system. The cybersecurity aspect is paramount as it imposes additional obligations on the manufacturers.

Chapter 4 contains an analysis of Client-side Scanning, which refers to scanning on devices such as smartphones with or without an online connection, and Human Rights Law.[14] It is also the only chapter that mentions surveillance in this thesis.[15] This does not mean that Client-side Scanning cannot be done in ways which conform better with existing privacy, safety, and security concepts. Furthermore, it is shown how Human Rights Law may concretely specify cybersecurity requirements for systems, contributing to the overarching picture.

Chapter 5 examines the draft EU Cyber Resilience Act,[16] which goes through which safety and security engineering principles should be used to regulate cybersecurity. The chapter analyses how the Act can regulate

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

[14]A small commentary on a EU proposal on Child Abuse protection related measures is also provided, which may end up mandating encryption which fails before it is implemented, that is, allowing any (not just law enforcement) to break it when deployed, breaching basic cybersecurity engineering principles.

[15]Elizabeth Stoycheff, Scott Burgess, and Maria Clara Martucci, "Online censorship and digital surveillance: the relationship between suppression technologies and democratization across countries" (2020) 23(4) Information Communication and Society 474 (Publisher: Taylor & Francis) ⟨https://doi.org/10.1080/1369118X.2018.1518472⟩; Yuval Yekutieli, "Is somebody watching you? Ancient surveillance systems in the southern Judean desert" (2006) 19(1) Journal of Mediterranean Archaeology 65.

[16]European Commission, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (2022).

cybersecurity, specifically in the context of Supply Chain Security.

The chapter asks the question of how the ecosystem of cybersecurity on a global or regional scale should be regulated. This is done through the lens of all types of supply chains, as failure to mitigate or prevent cyberattacks in any links of the chain could cause a failure of the entire system. The chapter adds a new way to define these attacks, which is a more direct version of existing definitions.

Critical infrastructure and the integrity of these complicated systems should be a top priority, but aside from decrees, contracts, and creative interpretations of existing rules, little *lex specialis* exists. Actual compliance and new solutions are recommended, and the chapter critically reviews measures to expropriate and implement relevant EU law in Danish, UK, and Irish law.

Chapter 6 rounds off the thesis with a set of conclusions.

The next chapter is the background for the thesis, including law and the legal areas used, as well as cybersecurity in both the computer science and engineering sense. This elaboration is necessary to understand all subsequent chapters and represents a further movement towards growing the academic intersection of law and computer science, as it includes both areas, and lets any lawyer, or any computer science scholar, read and understand what is done and why throughout the thesis.

The analysis is carried out through a multi- or interdisciplinary methodological lens that marries law, cybersecurity, and engineering, but this varies between each chapter; some will be interdisciplinary, while others will be multidisciplinary.[17]

[17]For more, see the overview in Chapter 2.

2 | Background and Methods

This chapter provides background and methodology for the thesis, first through law, starting with an introduction to the idea of regulation, and a short overview of each legal area applied. The latter consists of Private Law, Public Law, and a collection of other areas. After this, an overview of cybersecurity in computer science and engineering is given, including non-digital security as the historical angle, and an explanation of engineering terms that appear throughout the thesis. Following these two, the methodologies used in the thesis are discussed, including the role of multidisciplinary or interdisciplinary methods. Finally, a brief overview of the methods applied in each chapter is included. As can be seen, there is both here and throughout the thesis a heavier focus on the legal side, but the cybersecurity and safety perspectives are necessary to understand the areas which need regulation and contribute to the conclusions of the chapters.

2.1 Law

Law as an academic discipline is one of the oldest in existence, with the classic trio of examples being Ancient Egyptian, Sumerian and Babylonian Law.[1] Vedic Legal Rules, which intermingled strongly with religion and

[1]Nico Van Blerk, "The Ancient Egyptians' "Religious World": The Foundation of Egyptian Law" (2019) 28(1) Journal for Semitics ⟨https://www.upjournals.co.za/index.php/JSEM/article/view/4389⟩; Fernanda Pirie, "Law as ritual: Evoking an ideal order" en (2024) 14(2) HAU: Journal of Ethnographic Theory 403 ⟨https://www.journals.uchicago.edu/doi/10.1086/730785⟩ accessed 24 September 2024. There have likely been many

philosophy, also existed in this same period.[2] Since its inception, law has regulated technology in the form of criminal law,[3] currency,[4] and land laws.[5]

The best known example is the Code of Hammurabi,[6] which contains many of the earliest showcases of punitive and civil settlement clauses.

An example from this code could be Law 48, which stipulates the use of debt-tablets. These can be washed in water if one's grain is destroyed by a storm, the harvest failed, or crops did not grow due to lack of water. This Law acts as a technology specific clause where unpaid obligations to a creditor is allowed to be negated within a narrow set of terms and must use the selected type of technology. Humans were needed in various roles to execute the rules, but specific units of measurement,[7] techniques,[8] technologies, seen in maritime regulation of ships and their specifications

---

other types of law before these three, but they have not been preserved.

[2]Werner Menski, "Sanskrit Law: Excavating Vedic Legal Pluralism" [2010] SSRN Electronic Journal ⟨http://www.ssrn.com/abstract=1621384⟩.

[3]Anthony Leahy, "DEATH BY FIRE IN ANCIENT EGYPT" (1984) 27(2) Journal of the Economic and Social History of the Orient; JJ Finkelstein, "Sex Offenses in Sumerian Laws" (1966) 86(4) Journal of the American Oriental Society 355 ⟨https://www.jstor.org/stable/596493?origin=crossref⟩; Kristin Kleber and Eckart Frahm, "A Not-so-Great Escape: Crime and Punishment according to a Document from Neo-Babylonian Uruk" (2006) 58(1) Journal of Cuneiform Studies 109 ⟨https://www.journals.uchicago.edu/doi/10.1086/JCS40025226⟩.

[4]We cannot always establish whether a concrete legal source dictates the type of currency, but it will become at least soft law, perhaps enforceable as *de lege lata*. This is one of the unique situations where archaeology can concretely describe legal rules, see Mahmoud Ezzamel and Keith Hoskin, "Retheorizing accounting, writing and money with evidence from Mesopotamia and ancient Egypt" (2002) 13(3) Critical Perspectives on Accounting 333 ⟨https://linkinghub.elsevier.com/retrieve/pii/S1045235401905003⟩; Richard Mattessich, "Accounting and the Input-Output Principle in the Prehistoric and Ancient World" (1989) 25(2) Abacus 74 ⟨https://onlinelibrary.wiley.com/doi/10.1111/j.1467-6281.1989.tb00222.x⟩. See also Benjamin Geva, "From Commodity to Currency in Ancient History–On Commerce, Tyranny, and the Modern Law of Money" (1987) 25(1) Osgoode Hall Law Journal 115.

[5]See Piotr Steinkeller, "The Renting of Fields in Early Mesopotamia and the Development of the Concept of" Interest" in Sumerian" (1981) 24(2) Journal of the Economic and Social History of the Orient.

[6]I have made use of King's translation, LW King (tr), Hammurabi's Code of Laws (1915).

[7]See Law 24 and the 16 other that mention mina.

[8]Such as medicinal techniques, see Law 220.

in Laws 234 - 240, and 275 - 276, and many legal terms[9] were already well defined in the Code.[10]

During the Middle Ages,[11] developments in law regarding ships and seafaring,[12] trade,[13] and Canon Law[14] also regulated which technology to be used,[15] and the early onset of patents and other types of intellectual property regulation.[16]

[9]Terms like neglect, Law 125, or accidents in 266 and 267.

[10]Other examples of technology specific legislation include aspects of the legal frameworks in Shang and Zhou China, see James D Sellmann, "On the Origin of Shang and Zhou Law" (2006) 16(1) Asian Philosophy 49 ⟨https://www.tandfonline.com/doi/full/10.1080/09552360500491866⟩.

[11]Many contemporary periods existed in same period as the Middle Ages, such as the Delhi Sultanate, Nara period in Japan or the Islamic Golden Age, but we omit examples from these sources for now. These all had regulation of technology too.

[12]Edda Frankot, "Medieval Maritime Law from Oléron to Wisby: Jurisdictions in the Law of the Sea" in Juan Pan-Montojo and Frederik Pedersen (eds), *Communities in European history : representations, jurisdictions, conflicts* (Edizioni Plus – Pisa University Press 2007); Richard W Unger, "Channelling violence at sea: States, international trade and the transformation of naval forces from the high Middle Ages to the age of steam" (2019) 31(2) International Journal of Maritime History 202 ⟨http://journals.sagepub.com/doi/10.1177/0843871419844875⟩.

[13]Colin Kaufman, "The Law of International Commercial Transactions (Lex Mercatoria)" (1978) 19(1) Harvard International Law Journal 58; I Treiman, "Escaping the Creditor in the Middle Ages" (1927) 43(2) Law Quarterly Review 230.

[14]John A Lorenc, "John of Freiburg and the Usury Prohibition in the Late Middle Ages: A Study in the Popularization of Medieval Canon Law" (Doctor of Philosophy, University of Toronto 2013).

[15]Liliane Hilaire-Perez and Catherine Verna, "Dissemination of Technical Knowledge in the Middle Ages and the Early Modern Era: New Approaches and Methodological Issues" (2006) 47(3) Technology and Culture 536 ⟨http://muse.jhu.edu/content/crossref/journals/technology_and_culture/v047/47.3hilaire-perez.html⟩.

[16]For perspectives on regulation of technology, see, e.g. William H(William Henry) TeBrake, "Taming the Waterwolf: Hydraulic Engineering and Water Management in the Netherlands During the Middle Ages" (2002) 43(3) Technology and Culture 475 ⟨http://muse.jhu.edu/content/crossref/journals/technology_and_culture/v043/43.3tebrake.html⟩.

Many of the same technology specific[17] regulatory themes from above continued in various jurisdictions in both early and late Modern Period.[18] But a big shift came during the Industrial Revolution,[19] where machines and other societally changing technologies needed to be regulated either directly, including the steam engine, and indirectly through all machines that made use of the power, such as power looms.[20] The regulation of these was done through explicit technology specific legislation, or indirectly through technology neutral.[21]

With the brief overview of the historical context of technology and law completed, we can move to the practical context of law. This requires a definition and explanation as to what constitutes regulation.

2.1.1 Regulation

This subsection explores the concept of how regulation should or functions in the context of this thesis. Explaining this is necessary to make sure that

[17] Part of the dichotomy of technology specific and technology neutral regulation, see Bert-Jaap Koops, "Should ICT Regulation Be Technology-Neutral?" in (2006); Chris Reed, "Taking Sides on Technology Neutrality" (2007) 4(3) SCRIPT-ed 263 ⟨http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp⟩ accessed 29 July 2023; Paul Ohm, "The argument against technology-neutral surveillance laws" [2010] Texas Law Review.

[18] "The Technology and Economics of Coinage Debasements in Medieval and Early Modern Europe: with Special Reference to the Low Countries and England", in John H Munro (ed), *Money in the Pre-Industrial World* (1st, Routledge October 2015) ⟨https://www.taylorfrancis.com/books/9781317321910/chapters/10.4324/9781315655383-8⟩; Carlo Belfanti, "Guilds, Patents, and the Circulation of Technical Knowledge: Northern Italy during the Early Modern Age" (2004) 45(3) Technology and Culture 569 ⟨http://muse.jhu.edu/content/crossref/journals/technology_and_culture/v045/45.3belfanti.html⟩; JH Baker, "English Law and the Renaissance" (1985) 44(1) Cambridge Law Journal 46.

[19] There is a gap in scholarship in English that detail this development outside of Common Law countries, even though these exists in a historical format.

[20] John S Lyons, "Powerloom Profitability and Steam Power Costs: Britain in the 1830s" (1987) 24(4) Explorations in Economic History.

[21] Lawrence M Friedman and Jack Ladinsky, "Social Change and the Law of Industrial Accidents" (1967) 50 Columbia Law Review 50; Ikechi Mgbeoji, "The Juridical Origins of the International Patent System: Towards a Historiography of the Role of Patents in Industrialization" (2003) 5(2) Journal of the History of International Law / Revue d'histoire du droit international 403 ⟨https://brill.com/view/journals/jhil/5/2/article-p403_7.xml⟩; Grant Gilmore, "From Tort to Contract: Industrialization and the Law" (1977) 86(4) The Yale Law Journal 788 ⟨https://www.jstor.org/stable/795645?origin=crossref⟩.

the reader understands that it differs from other definitions, and for the familiarity with the concept to be guaranteed.

The section is a preface to the methodological limits which law brings when discussing the idea of regulation.This concept is central in the regulation of technology, including any discussion of law and cybersecurity, as the latter can cause financial[22] and physical damage[23] if it fails. Notable authors on regulation as a term include *Black*,[24] *Cohen*,[25] and *Brownsword*.[26] I will start by explaining why I am not using any of the ideas these three have presented in the selected papers.

Black applies the idea of including legal sources traditionally not seen as those who regulate,[27] and considers them important in a post-regulation world,[28] while also showing both the problem and the solution in the form of self-regulation.[29] Self-regulation exists both as a hurdle to those that

[22]Fawaz Alharbi and others, "The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia" (2021) 21(20) Sensors 6901 ⟨https://www.mdpi.com/1424-8220/21/20/6901⟩.

[23]David J Slotwiner and others, "Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians—Proceedings of the Heart Rhythm Society's Leadership Summit" (2018) 15(7) Heart Rhythm e61 (Publisher: Elsevier Inc.) ⟨https://doi.org/10.1016/j.hrthm.2018.05.001⟩.

[24]"Critical Reflections on Regulation", in Julia Black and Fiona Haines (eds), *Crime and Regulation* (1st edn, Routledge November 2017); J Black, "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World" (2001) 54(1) Current Legal Problems 103 ⟨https://academic.oup.com/clp/article-lookup/doi/10.1093/clp/54.1.103⟩.

[25]Julie E Cohen, "The Regulatory State in the Information Age" (2016) 369(2) Theoretical Inquiries in Law; Shameek Konar and Mark A Cohen, "Information As Regulation: The Effect of Community Right to Know Laws on Toxic Emissions" (1997) 32(1) Journal of Environmental Economics and Management 109 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0095069696909559⟩.

[26]Roger Brownsword, *Rethinking Law, Regulation, and Technology* (Edward Elgar 2022); Roger Brownsword, "Artificial Intelligence and Legal Singularity: The Thin End of the Wedge, the Thick End of the Wedge, and the Rule of Law" in Simon Deakin and Christopher Markou (eds), *Is Law Computable?: Critical Perspectives on Law and Artificial Intelligence* (Hart Publishing 2020) ⟨http://www.bloomsburycollections.com/book/is-law-computable-critical-perspectives-on-law-and-artificial-intelligence⟩; R Brownsword, "The shaping of our on-line worlds: getting the regulatory environment right" (2012) 20(4) International Journal of Law and Information Technology 249 ⟨https://academic.oup.com/ijlit/article-lookup/doi/10.1093/ijlit/eas019⟩.

[27]Black (n 24).

[28]Similar to those who oppose the idea in Legal Positivism that all law is from the state alone.

[29]Black (n 24) 124 - 128.

want to control via regulation, as it functions by both complying, circumventing, and controlling the behaviour internally of companies and individuals, but also works as a solution to the problems which regulation may have. The latter comes through the notion of any regulation mostly happening through self-regulation.[30] In this thesis, this idea is very supported, as many aspects of cybersecurity happen internally within companies and developers themselves, following standards and guidelines only happen if these parties choose to, outside of special areas such as medical devices.[31] The notion of decentralized regulation is not adopted further in this thesis, as the risk of circumvention, ignorance, or other inaction exists, if there is no central actor to control or otherwise encourage compliance.[32] This also plays into why co-regulation[33] is not suggested either. Co-regulation is the idea of giving responsibility for both shaping and putting the effects of regulation into practice,[34] between public and private parties. Because of the deliberately shared nature, the issues of circumvention and malpractice may be greater.

Cohen introduces the idea that regulators should possess other roles,[35] specifically entrepreneur,[36], auditor[37] and manager.[38] This distinction lets legal analysis understand the various roles which regulators will delegate

[30]ibid 125.

[31]For more on the cybersecurity requirements and enforcement mechanisms that differ, see Chapter 3 and 5 of this thesis.

[32]This is not simplify things, as there is room for it in how *Black* describes it, but there is a large different between defining your whole system by not being central, versus being central, in terms of how it is structured and deployed in practice. For more, see JG Allen, "Bodies without Organs: Law, Economics, and Decentralised Governance" (2020) 4(1) Stanford Journal of Blockchain Law & Policy.

[33]Linda Senden, "SOFT LAW, SELF-REGULATION AND CO-REGULATION IN EUROPEAN LAW: Where Do They Meet?" (2005) 9(1) Electronic Journal of Comparative Law.

[34]Dennis D Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation" (2011) 34(2) Seattle University Law Review, 4.

[35]Cohen (n 25).

[36]ibid 396.

[37]ibid 402.

[38]ibid 410.

or give themselves, and can explain various constructions of private-public collaboration, use of standards as soft regulation, and control with budget and micromanagement. These describe the rather combined role which real regulation takes in most countries, and in cybersecurity, this is seen through the collaboration which big corporations have with governments regarding security, or the way which public investments can lead to the entrepreneur attributes which *Cohen* describes. However, this thesis will not make use of these ideas further, as they only partially answer the complexity which regulation of anything brings, do not highlight the role which it would play if it was brought to court, and makes use of the idea of nudging or sludging, techniques which at best are underdeveloped, or at worst are unfounded.[39]

Brownsword details characteristics which should be used to create the right regulatory environment,[40] which consists of the following concepts: Regulatory prudence, regulatory legitimacy, regulatory effectiveness, and regulatory connection. Regulatory prudence entails predicting potential failures and risks imposed by the technology used or regulated. Regulatory legitimacy consists of procedural legitimacy, that is, the means which legitimacy is established also considers the way to reach it - legitimacy of regulatory purposes and standards, and legitimacy of regulatory instruments. Regulatory effectiveness considers the regulators and subjects, and whether either hinder implementation. Regulatory connection refers to the connection technology has with the means, authorities, or the regulation itself, including connection and disconnection between technology and regulation. While these concepts can serve as inspiration, they all de-

[39]Magda Osman, Nudges: four reasons to doubt popular technique to shape people's behaviour (2022) ⟨https://theconversation.com/nudges-four-reasons-to-doubt-popular-technique-to-shape-peoples-behaviour-174359⟩.

[40]Brownsword (n 26).

scribe already well known ideas in law,[41] including regulatory connection, which is better described as the issue of technology neutral or technology specific regulation of technology.[42] This thesis will therefore not make use of any of these concepts, even if they do lend themselves well for further research specifically regarding cybersecurity.

The ability to dictate the behaviour of other individuals is the study of other sciences,[43] but the role which law has in this does not enjoy universal agreement. One approach has been to describe and attest parts of law as norms,[44] the hierarchy of norms is well known here and in other disciplines,[45] and while these can provide temporary answers,[46] they do not inherently unveil what makes law provide the measures to regulate. This can be explained in the following manner. Norms will illustrate sources and means to regulate, and one will derive the norms from the rules in practice, but any norm must be governed by a higher norm. The end of the usefulness of describing regulation as norms therefore becomes the situ-

[41] Prudence can be considered the spirit or the reasoning behind developing regulation of an area, legitimacy is such a wide and complicated term that it is better left out, effectiveness is better explored empirically and by the design of law. All of these can be seen better reflected in places such as Kelsen's Pure Theory of Law, Hans Kelsen, "Pure Theory of Law, The - Its Method and Fundamental Concepts" (1934) 50(4) Quarterly Review.

[42] Koops (n 17).

[43] Aitor Jiménez González, "Law, Code and Exploitation: How Corporations Regulate the Working Conditions of the Digital Proletariat" (2022) 48(2) Critical Sociology 361 ⟨http://journals.sagepub.com/doi/10.1177/08969205211028964⟩; Radha D'Souza, "When Unreason Masquerades as Reason: Can Law Regulate Trade and Networked Communication Ethically?" in *The Handbook of Communication Ethics* (Routledge 2011); Anne Griffiths, "Law, Space, and Place: Reframing Comparative Law and Legal Anthropology" (2009) 34(02) Law & Social Inquiry 495 ⟨https://www.cambridge.org/core/product/identifier/S0897654600006067/type/journal_article⟩.

[44] Griffiths (n 43); Annika Tahvanainen, "Hierarchy of Norms in International and Human Rights Law" (2006) 24(03) Nordic Journal of Human Rights 191 ⟨https://www.idunn.no/ntmr/2006/03/hierarchy_of_norms_in_international_and_human_rights_law⟩.

[45] JAC Salcedo, "Reflections on the Existence of a Hierarchy of Norms in International Law" (1997) 8(4) European Journal of International Law 583 ⟨https://academic.oup.com/ejil/article-lookup/doi/10.1093/oxfordjournals.ejil.a015608⟩; Dinah Shelton, "Hierarchy of Norms and Human Rights: Of Trumps and Winners" (2002) 65(2) Sasktchewan Law Review; Franz Merli, "Principle of Legality and the Hierarchy of Norms" [2015] Southern California Law Review.

[46] Karl-Heinz Ladeur, The Theory of Autopoiesis as an Approach to a Better Understanding of Postmodern Law (EUI Working Papers, 1999).

ation where the norms of a constitution or international law is analysed, and *no* norm above it to describe how it is controlled or understood exists. This metaphysical discussion of assumed attributes of actual legal rules is the basis of *Dworkin's* criticism of legal positivism.[47]

Turning to Bad Man's law,[48] the perspective of the Bad Man who wants to circumvent or not comply, to his own advantage, is necessary to show that regulation needs incentive or compliance structures,[49] and to highlight the practical problems that non-lawyers face constantly when realising their position in a regulatory system. Bad Man's law can narrowly be defined as pure circumvention or loophole analysis and usage, which does not answer how regulation occurs, only how it can be avoided or maliciously complied with. Good regulation must therefore prevent Bad Man's law from being the optimal solution.

Regulation can be defined in several ways, including legal instrument, combination of all laws affecting anyone at any time, or based on relationships and divided in this manner.[50]

Building on the tradition of Scandinavian Legal Realism, this thesis employs the idea that regulation is expressed by power projection. It can be defined as: *regulation is the medium by which power is projected onto others*.[51] The simplicity of the concept allows for clear definitions for those that enforce and create the law, and the regulated. Doing so, the identities of all parties, and the scrutiny and understanding needed for the actual

[47]Ronald Dworkin, *Law's Empire* (1st edn, Harvard University Press 1986).

[48]Holmes' idea of Bad Man's law is from a speech from 1897, but has become timeless because of its practical usage, see, e.g., Marco Jimenez, "Finding the Good in Holmes's Bad Man" (2011) 79(5) Fordham Law Review 2069.

[49]William Twining, "The Bad Man Revisited" [1972] Cornell Law Review 39 ⟨https://www.taylorfrancis.com/books/9781351543767/chapters/10.4324/9781315086323-3⟩.

[50]David Levi-Faur, "REGULATION & REGULATORY GOVERNANCE" in *Handbook on the Politics of Regulation* (Elgar 2011) 4.

[51]This definition follows one of the core concepts of Scandinavian Legal Realism, see Alf Ross, *Om Ret og Retfærdighed* (2nd edn, Gyldendal 2013) 99-105, and equivalent in the translated version.

compliance are made clear.[52]

In this sense, this thesis consists of the doctrinal legal analysis done to uncover the state of the law and means to circumvent obligations and not comply with the spirit of the law. For more on the methodology specifically, outside of the discussion of regulation as done here, see later in 2.3.1.

The definition of regulation above shows which criteria must be fulfilled for full regulation or compliance through power projection, something which the engineering sciences focus on, but there is one important distinction to make. The degree to which regulation is fulfilled or happens is not the same as the one which the authority of the regulation wished it to be *per se*.[53] Coincidentally, this is a feature shared with statistics and its usage in engineering. Tools and means to express statistics, such as gradients, normal distributions, and likelihood analysis, all have this in common with regulation.[54]

Empirical studies on how efficient legislation is do exist,[55] but we lack concrete answers that thoroughly explain how we may enforce regulation perfectly or close to, without delving into concepts like code as law.[56] The concept can be traced back to *Lex Informatica*,[57] meaning that code as soft law can regulate human behaviour.[58] This thesis does not make use of

[52]However, empirical studies on compliance, to uncover whether the power projection is effective, are not deployed in this thesis. But this is a direction which the potential future work can take regarding cybersecurity, see Chapter 5.

[53]This can be seen as a teleological issue with regulation, the clash between the regulator and the regulated subject.

[54]And perhaps likelihood in general, with all its faults, share this commonality with the problem of regulation, see Robert F Nau, "DE FINETTI WAS RIGHT: PROBABILITY DOES NOT EXIST" (2001) 51 Theory and Decision 89 ⟨https://link.springer.com/article/10.1023/A:1015525808214%7B%5C#%7Dciteas⟩.

[55]Such as Konstantinos Stylianou and Marios Iacovides, "The goals of EU competition law: a comprehensive empirical investigation" [2022] Legal Studies 1 ⟨https://www.cambridge.org/core/product/identifier/S0261387522000083/type/journal_article⟩.

[56]Lessig (n 10).

[57]Joel R Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology" [1997] (76) Texas Law Review.

[58]Primavera De Filippi and Samer Hassan, "Blockchain technology as a regulatory

the terminology, because it would require insight into the systems which consist of the relevant *Lex Informatica* for a given situation, and because it would limit or compartmentalise the relevant soft law (algorithms, or an understanding of systems) and the given positively defined law.

A relevant and noteworthy approach to the regulation of technology is the (regulatory-technical) tools in use. Of specific interest for this thesis, is the dichotomy between technology neutral and technology specific regulation. Technology neutral regulation entails that the legislation does not distinguish between diverse types of technology used or which otherwise play a role. On the other hand, technology specific legislation seeks to only regulate defined types of technology, allowing for more detailed regulation. There are various views on which type is the most relevant,[59] but both have their uses, as illustrated with legislation like the GDPR, which is technology neutral, and telecommunication legislation,[60] which tends to be technology specific. It also showcases how the choice of subject determines which kind of possibilities are open when designing tools for regulation, a theme which continues throughout this thesis.

The next subsections will give an overview of the different legal areas which the thesis makes use of. It starts out with Private Law, due to its role for individuals and legal entities, as it regulates relationships and many financial rights between them and the state.

technology: From code is law to law is code" [2016] First Monday ⟨https://firstmonday.org/ojs/index.php/fm/article/view/7113⟩ accessed 2 February 2024.

[59]Koops (n 17); Reed (n 17); Ohm (n 17); Marco Almada, "Two dogmas of technology-neutral regulation" [2024] .

[60]Such as Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ LL321/36.

2.1.2 Private Law

Due to the role which Private Law always plays when regulating technology, including cybersecurity, Contract and Torts need explanation, though they are not all which Private Law constitutes. The relevant Private Law which this thesis makes use of is only Danish, including the Law of Reimbursement Responsibility.[61]

Danish Law for Chapter 3 was chosen because of its role within Scandinavian Law as a legal family, where it represents aspects of both Civil Law and Common Law at the same time, while having unique attributes which none of those have. It also highlights the unique Private Law approaches, which are rarely covered due to the language barrier, and which are equivalent to what can be found in both Norwegian, Swedish, Icelandic, and Finish Law, allowing Danish Law to represent a multitude of legal systems at the same time.

Private Law is characterised as regulating and forming the relationships between private parties.[62] This includes those seen between citizens, legal entities (companies), the state as a private party to others, or any combination in-between. Some systems will consider civil litigation to be contained elsewhere, but for this thesis, it is included here as well. Private Law encompasses other elements than contractual relationships and consequences. These include detailed rights in many shapes, such as property, from real estate to intellectual property, but also rights for creditors and debtors when matters must be settled in court. The latter, while not relevant for thesis, will overlap sharply with Public Law regarding how their

[61] LBK nr 1070 af 24/08/2018.

[62] See primarily Jens Evald, *Juridisk teori, metode og videnskab* (2nd, Jurist- og økonomforbundets Forlag 2020) 24. Otherwise see Randy E Barnett, "Foreword: Four Senses of the Public Law-Private Law Distinction" (1986) 9(2) Harvard Journal of Law & Public Policy 11. On the contrary, see Carol Harlow, "Public and Private Law: Definition without Distinction" (1980) 43(3) Modern Law Review 241, Ross (n 51) 263-267.

rights can be enforced, and may overlap with the criminal sphere too.[63]

The next small section details some background on how the term Contract is understood and serves as the small background and introduction to its usage throughout the thesis.

Contract

Contracts have played a major role in cybersecurity so far,[64] through procurement and voluntary collaboration, and by requirements for systems imposed through contracts.[65] The latter, through Software Bill of Lading[66] and other similar procurement instruments, is important because it imposes technical requirements via obligations similar to those seen in the shipping and transport industry. The downside of regulating cybersecurity through contracts is that unless enforced in court or by authorities, there is no guarantee that their contents will ever affect anything.[67] Software Bill of Lading is closer to a better solution, as these are enforced through procurement, but this comes with the caveats which procurement in general bring.

Despite this, contracts play a vital role in every society. No legal system can function without them, and they create the basis of informal trading at a market without receipt, coffee at your local café, mortgage agreements, employment, procurement and so on.

Various legal systems have different perspectives, some will only work

[63] Barnett (n 62); Harlow (n 62).

[64] John D Tangney, *History of Protection in Computer Systems:* (techspace rep, Defense Technical Information Center 1980) ⟨http : / / www . dtic . mil / docs / citations / ADA108830⟩; James P Anderson, *Computer Security Technology Planning Study. Volume 2:* (techspace rep, Defense Technical Information Center 1972) ⟨http://www.dtic.mil/docs/citations/AD0772806⟩.

[65] Seth Carmody and others, "Building resilient medical technology supply chains with a software bill of materials" (2021) 4(1) npj Digital Medicine 34 ⟨http://www.nature.com/articles/s41746-021-00403-w⟩.

[66] ibid.

[67] This is a general weakness of Private Law.

within the contract, usually Common Law, while others combine the agreement with background law which exist outside the contract, usually both Civil Law and Scandinavian Law.[68] Individual jurisdictions within those overarching comparative categories may have more in common with the opposite or vice versa, and in-depth understanding and analysis of each system is necessary to identify the law surrounding and concerning the contract. Nevertheless, we can break down the idea of a contract as follows:[69]

1. A contract is a legal instrument between two or more parties.

2. A contract must be enforceable, otherwise is only has the value of guidance.

3. A contract can be limited, unlimited or undefined, but step 2 enables it to be either. The same applies to other specific conditions. This includes criteria of form, delivery, and understanding.

This way, contracts can serve as the delivery of services, goods, ideas, and placing someone into a certain framework, which is done in various ways throughout the thesis.
In the next small section, some details surrounding the enforcement of contracts and recovery of damages through Torts are detailed.

Torts and Reimbursement

Torts is a mechanism to compensate, balance, and otherwise direct methods for damages, whether defined in contracts or not. Breaches of contract,

[68] These definitions are included for the sake of simplification, for more, see K Zweigert and H Kötz, *An Introduction to Comparative Law* (Third Edition, Oxford University Press 2011).

[69] These definitions have similarities to the definition proposed in Bernhard Gomard, Hans Viggo Godsk Pedersen, and Anders Ørgaard, *Almindelig kontraktsret* (4th, Jurist- og økonomforbundets Forlag 2015). The difference lies in the aim, which here is more universal, and not an attempt to describe contracts in one jurisdiction.

in particular those relating to Product Liability, are one of the focal areas of Chapter 3. This includes the concept of Reimbursement, which is similar to Torts in Common Law, but not entirely, and therefore must be treated differently.[70]

Tort is ancient, and was practiced in several ways in the past, expressed through, e.g., Criminal Law in Ancient Egypt[71] to now being a Private Law mechanism and enforced through courts[72] or arbitration.[73] It is both used in accidents, contractual breaches, and more, and has different conditions and attributes attached to it depending on jurisdiction and practical context, as damage in different situations may require unique parameters to judge and understand.[74] Torts generally require quantifiable damage, identified parties and a link of causality between the incident and the damage which it is claimed it caused.

There is little case law regarding tort or reimbursement cases where cybersecurity has played a significant role. Outside of this thesis, there is a range of literature which describes what may happen, but these rarely go into further detail in terms of the cybersecurity involved.[75]

Now that the necessary background for the use of Private Law in the thesis has been established, we can move on to the discussion of Public Law.

[70]It can be explained as differences in procedure and necessary steps before Reimbursement can be applied in court.

[71]Russ VerSteeg, "Law in Ancient Egyptian Fiction" (1994) 24(1) Georgia Journal of International and Comparative Law 63.

[72]Enforceability through courts is important to keep in mind, as Chapter 3 show that the same principles that can be seen in Torts, can be used in Public Law settings as well, albeit quite specific, but to the great benefit of the citizen.

[73]In some jurisdictions, arbitration is facilitated by courts and private entities, in others it is only the latter.

[74]See, e.g., Saul Levmore, "Rethinking Comparative Law: Variety and Uniformity in Ancient and Modern Tort Law" (1986) 61(2) Tulane Law Review 235; Bjarte Askeland and others, *Basic Questions of Tort Law from a Comparative Perspective* (Jan Sramek Verlag 2015) ⟨https://library.oapen.org/handle/20.500.12657/33062⟩.

[75]Exceptions to this include Mario Martini and Carolin Kemper, "Cybersicherheit von Gehirn-Computer-Schnittstellen" [2022] International Cybersecurity Law Review (ISBN: 1281121339).

2.1.3 Public Law

The associations of the state regulating individuals through decrees,[76] laws and establishing courts have been the standard way of thinking, but much has changed since the start of the last century.[77] This thesis works with a general concept of Public Law that covers all types of regulation given by the state. It focuses largely on Administrative Law, and product regulation. Administrative Law is the legal system which surrounds the state's institutions, service, or physical infrastructure of citizens and access to council or communal resources.[78]

Product regulation, be it EU or in a national legal system, refer to obligations for manufacturers and rights for the authorities which oversee them.[79] General Public Law used in this thesis include implementations of EU law, which are detailed in the next subsections.[80] One outlier from this is the act of complaint and reimbursement access in the health-sector,[81] which plays a role in Chapter 3.

Administrative law plays an ever increasing role, in as different jurisdictions as the US or Denmark,[82] with increased usage of the state as a private party or hybrid structures through private parties partially overtaking the public role of the State.[83] This includes cases such at private companies

[76] Ross (n 51) 81.

[77] Including the acknowledgement of the role which self-regulation plays, see Black (n 24).

[78] Jennifer Cobbe, "Administrative law and the machines of government: Judicial review of automated public-sector decision-making" (2019) 39(4) Legal Studies 636.

[79] Geraint Howells, "Product Liability – A History of Harmonisation" in *Product Liability in Comparative Perspective* (Cambridge University Press 2005).

[80] One of these is the Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L277, which is mentioned once.

[81] LBK nr. 995, 14/06/2018.

[82] They may have more in common than initially thought however, see Francesca Bignami, "From Expert Administration to Accountability Network: A New Paradigm for Comparative Administrative Law" (2011) 59(4) American Journal of Comparative Law 859 ⟨https://academic.oup.com/ajcl/article-lookup/doi/10.5131/AJCL.2010.0031⟩.

[83] RM Bertens and RAA Vonk, "Small steps, big change. Forging a public-private

being mandatory to as fundamental issues as tax filing,[84] or automated-decision-making of administrative decisions by software owned and run by corporations[85] and so on.

Public Law otherwise regulates every aspect of the state, the state's interactions with individuals, rights, and obligations of individuals and even non-human actors.

Like Private Law, Public Law now covers a wide reaching amount of different themes.[86] One of them is cybersecurity, which has been regulated in Public Law in various jurisdictions considering critical infrastructure,[87] where entities such as the EU have required it.[88] Outside of Public Law, there exists standards and guidance which, through contracts or otherwise, serve as *de facto* requirements for encryption and other cybersecurity aspects.[89] Public Law may then refer to these, or in some jurisdictions, simply just require "state of the art",[90] which means the best possible for the level of company or state organ, which is supposed to implement cybersecurity, often in direct reference to a specific standard.

Public Law plays no role in the rest of the chapters in its generic and ad-

---

health insurance system in the Netherlands" (2020) 266 Social Science & Medicine 113418 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0277953620306377⟩.

[84]Kacey Marr, "You're Only as Good as Your Tax Software: The Tax Court's Wrongful Approval of the Turbotax Defense in Olsen v. Commissioner" (2012) 81(2) University of Cincinnati Law Review 709.

[85]Cobbe, "Administrative law and the machines of government: Judicial review of automated public-sector decision-making" (n 78).

[86]Evald (n 62) 23.

[87]John J Chung, "Critical Infrastructure, Cybersecurity, and Market Failure" (2018) 96(2) Oregon Law Review 441.

[88]E.g., in finance, Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert, "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation" (2019) 35(6) Computer Law & Security Review 105336 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364919300512⟩.

[89]Whether they function is another matter, see Aaron Clark-Ginsberg and Rebecca Slayton, "Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards" (2019) 46(3) Science and Public Policy 339 ⟨https://academic.oup.com/spp/article/46/3/339/5184558⟩.

[90]Hamdi Kavak and others, "Simulation for cybersecurity: state of the art and future directions" (2021) 7(1) Journal of Cybersecurity 1 ⟨https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyab005/6170701⟩.

ministrative nature. However, through specific administrative rules and use of authorities, it is employed to solve issues which Private Law cannot in Chapter 5. On top of this, the specialised fields below play various roles in thesis as well.

Human Rights Law is covered later in this chapter, though Human Rights Law can also be considered an area of law beneath the Public Law mantle. The next section is a specialised area of Public Law, which is frequently used as reference point and inspiration in various places of the thesis but is not a core part of it. Despite this, it still requires its own section to justify and explain its role, regardless of its size, as it is often from this simple cybersecurity requirements stem.

Data Protection

The area of Data Protection exists under Public Law, due to its product regulatory function. Data protection as a term requires a succinct explanation of privacy, as this is one of the core protection areas for the field, though it is not everything. Data Protection should be understood in its literal sense, as protection of data and information security, which is also attached to the broader field of cybersecurity.[91] Since the inception of the field in 1970 in the State of Hesse in Germany,[92] the practice surrounding the protection has also been included in the definition.

Privacy has not always been a right,[93] outside of encryption or secrecy of communication, which has existed since ancient times.[94] But with its

[91] It is worth noting that information security only includes protection of information, whereas cybersecurity involves all security.

[92] Fred H Cate, "The EU Data Protection Directive, Information Privacy, and the Public Interest" (1995) 80(3) Iowa Law Review.

[93] Jan Holvast, "History of Privacy" (2009) 298 FIP Advances in Information and Communication Technology; Irwin R Kramer, "The Birth of Privacy Law: A Century since Warren and Brandeis" (1990) 39(3) Catholic University Law Review 703.

[94] John F Dooley, "The Black Chambers: 1500–1776" in *History of Cryptography and Cryptanalysis* (Series Title: History of Computing, Springer International Publishing 2018) ⟨http://link.springer.com/10.1007/978-3-319-90443-6_3⟩.

recent development came the notion of protecting gathered data,[95] applying mainly to individuals, and specifically when the data is personal in a EU context through the former Data Protection Directive[96] and the GDPR. The forefront for this has been in Europe,[97] but with Data Protection came notions as to what kinds of cybersecurity are necessary to protect it, as the assumed "protection" would otherwise not be possible.

In a GDPR[98] context,[99] the Regulation cannot be followed if the security of the servers of devices which analyse the data is poor, so indirect standards and notions were created to accommodate these necessary security requirements to protect personal data.[100] On the contrary, the enforcement of GDPR has been characterised as lacklustre,[101] which could cause worse cybersecurity due to lack of actions to ensure it.

Data Protection sees use in the thesis in the form of comparisons to the GDPR. It is not used as the central basis of any of the chapters.

The next section involves the most important legal area for the thesis, the Public Law based regulation of cybersecurity.

[95] This surprisingly includes non-personal data, see Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L303.

[96] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281.

[97] Earliest with The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Convention 108, 1981.

[98] Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1. There is also one mention of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L119/89.

[99] Sara Degli-Esposti and Ester Mocholí Ferrándiz, "A Year after GDPR: Cybersecurity is the Elephant in the Artificial Intelligence Room" (2021) 32(1) European Business Law Review 24.

[100] Depending on jurisdictions, this was the case in the Data Protection Directive as well.

[101] Garrett Johnson and Scott Shriver, Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR (2019) ⟨https://www.ssrn.com/abstract=3477686⟩.

Cybersecurity

Cybersecurity is a specialised branch of security of digital systems, which has evolved and is now far more detailed and complicated than its originator. The notion of regulating cybersecurity came from early ideas in Cybernetics.[102] As a separate regulatory area, cybersecurity has been developed thoroughly in both German[103] and Polish Law,[104] taking inspiration from existing legislation on necessary standards and needed technological implementations, though with consequences in the form of inadequate wording, lacking enforcement and more. The amount of literature concerning non-English jurisdictions is low, meaning that other great sources usually discuss the regulation of cybersecurity in US[105] or UK Law,[106] where it is less developed and relies far more on soft law, and secret or at least unclear enforcement structures.

Enforcement is central, as most of the major corporations which affect our daily lives (in a EU context) reside in countries, such as the US, who do not necessarily have extensive requirements for cybersecurity outside of what can be forced upon the corporations, and whose authorities must

[102]Cybernetics inspired Computer Science in several ways, see Stuart A Umpleby, "A Short History of Cybernetics in the United States" (2008) 19(4) Österreichische zeitschrift für geschichtswissenschaften 28. Cybernetics may continue to serve as inspiration, Deborah Cernauskas and Andrew Kumiega, "Back to the future: Cybernetics for safety, quality and cybersecurity" (2022) 29(3) Quality Management Journal 183 ⟨https://www.tandfonline.com/doi/full/10.1080/10686967.2022.2083035⟩; Antonio Roque, Kevin B Bush, and Christopher Degni, "Security is about control: insights from cybernetics" (ACM April 2016) ⟨https://dl.acm.org/doi/10.1145/2898375.2898379⟩.

[103]Martini and Kemper (n 75).

[104]Tomasz Zdzikot, "Cyberspace and Cybersecurity" in *Cybersecurity in Poland* (2022).

[105]Matthew Ashton, "Debugging the Real World: Robust Criminal Prosecution in the Internet of Things" (2017) 59(805) Arizona Law Review ⟨http://arizonalawreview.org/pdf/59-3/59arizlrev805.pdf⟩; Justin Hurwitz, "Cyberensuring Security" (2017) 49(5) Connecticut Law Review; Justine Morris, "Surveillance By Amazon: The Warrant Requirement, Tech Exceptionalism, & Ring Security" (2021) 27(1) Boston University Journal of Science and Technology Law 237 (ISBN: 3600279793).

[106]Kristan Stoddart, "Live Free or Die Hard: U.S.-UK Cybersecurity Policies" (2016) 131(4) Political Science Quarterly 803 ⟨https://onlinelibrary.wiley.com/doi/10.1002/polq.12535⟩.

keep them accountable.[107]

In essence, cybersecurity as Public Law should entail requirements for design, structure, behaviour, and resilience measures. As mentioned earlier, this thesis explores whether this actually occurs, within different contexts in each chapter.

The legislation used regarding the regulation of cybersecurity in the thesis, from the European Union, is:

- The NIS1 Directive.[108]
- The NIS2 Directive.[109]
- The Proposed Cyber Resilience Act.[110]
- The Cybersecurity Act.[111]
- The Proposed Cyber Solidary Act.[112]

Chapter 5 uses three different types of implementations of the NIS1 Directive from national law, which are:

[107]This thesis does not discuss this in further detail, for more, see Jeff Kosseff, "Upgrading Cybersecurity Law" [2023] Houston Law Review; Jeff Kosseff, "Defining Cybersecurity Law" (2018) 103(3) Iowa Law Review; Jeff Kosseff, "Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System" (2016) 19(2) Chapman Law Review. Note that this is not a discussion of differences in enforcement or whether EU companies are much better, merely that there are classical problems regarding the federal structure of the US that have not been solved regarding cybersecurity.

[108]Directive (EU) 2016/745 of the European Parliament and of the Council of 5 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L194/1

[109]Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), [2022] OJ L333/80.

[110]Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final, 2022/0272 (COD).

[111]Regulation 2019/81 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), [2019] L 151/15.

[112]Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, COM(2023) 209 final, 2023/0109 (COD).

- NIS-Loven[113] in Danish Law.
- The Network and Information Systems Regulations 2018[114] in UK Law.
- Statutory Instrument No. 360 of 2018 in Irish Law.

Danish, Irish, and UK Law were picked in Chapter 5 because they represent three different ways to implement EU Law, and because Irish and UK Law are both closely related, and yet, have diverged significantly since Ireland's Independence.[115] Furthermore, they make a strong contrast to the Scandinavian Law example (Danish Law).

Moving on from technical requirements to a section concerning a publicly regulated area, product regulation, which is also expressed heavily in Private Law in the form of litigation. But its roots currently reside in Public Law in an EU context, hence its placement here.

Product Regulation

This thesis centres heavily around the regulation of products. This type of legislation targets the manufacturers, and the authorities which must support, control, and create market surveillance around the products.

The following legislation in this theme is used in the thesis are:

[113] LOV nr 436 af 08/05/2018.

[114] Statute No. 506, 2018.

[115] Bryan Fanning, Weronika Kloc-Nowak, and Magdalena Lesińska, "Polish migrant settlement without political integration in the United Kingdom and Ireland: a comparative analysis in the context of Brexit and thin European citizenship" (2021) 59(1) International Migration 263 ⟨https://onlinelibrary.wiley.com/doi/10.1111/imig.12758⟩ accessed 19 February 2023; Daniel Gilling and others, "Powers, liabilities and expertise in community safety: Comparative lessons for 'urban security' from the United Kingdom and the Republic of Ireland" (2013) 10(3) European Journal of Criminology 326 ⟨http://journals.sagepub.com/doi/10.1177/1477370813482612⟩ accessed 19 February 2023; Cormac Behan, "Embracing and Resisting Prisoner Enfranchisement: A Comparative Analysis of the Republic of Ireland and the United Kingdom" (2014) 11 IRISH PROBATION JOURNAL.

- The Medical Device Directive.[116]
- The Medical Device Regulation.[117]
- The Product Liability Directive.[118]
- The AI Act Proposal.[119]

A few words on the latter are needed to flesh out why it is placed here, as it could also have had its own section.

Product Liability and Regulation has a rather short history. Depending on framework and interpretation, it either started as fleshed out safety legislation,[120], an extension of principles from contract and obligation law,[121] or it started with the concept of consumerism.[122] Some jurisdictions developed and used this early in the twentieth century,[123] while many others only started towards the end.[124]

Medical Device Regulation, and Product Liability are the focal points of Chapter 3. The focus is principally on the implementation and understanding of it in EU law, but also discusses how a state like Denmark, which has

[116]Council Directive 93/42/EEC of 14 June 1993 concerning medical devices [1993] OJ L169/1.

[117]Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L117/1.

[118]Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L210/29.

[119]Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM/2021/206 final.

[120]PN Legh-Jones, "Products Liability: Consumer Protection in America" (1969) 27(1) The Cambridge Law Journal 54 ⟨https://www.cambridge.org/core/product/identifier/S0008197300088905/type/journal_article⟩ accessed 18 December 2023.

[121]Fred W Morgan and Karl A Boedecker, "A historical view of strict liability for product-related injuries" (1996) 16(1) Journal of Macromarketing 103.

[122]Starting with *MacPherson v. Buick Motor Co.* in the US, David W Leebron, "eeb" [1990] (3) Annual Survey of American Law.

[123]An example of this is Danish law, see Mads Bryde Andersen and Joseph Lookofsky, *Lærebog i obligationsret* (4th, vol 1, Karnov Group 2010).

[124]Howells (n 79). Examples are any EU member state which had no existing system in place before the Product Liability Directive.

practiced Product Liability for more than one hundred years enabled litigation with slightly different tools. All of these discussions are done in the light of adversarial attacks on medical devices within cybersecurity.

Product Liability constitutes a developing interesting area going forward, as the amount of damage which adversarial attacks cause increases and aligns well with the new proposals from the European Commission to adapt the Product Liability area for the new types of products present.[125]

There are also a few mentions, but not usage, of some other EU product legislation, which are the Food Hygiene Directive,[126] the Jurisdiction Directive,[127] and the In vitro Medical Device Regulation.[128]

In the next couple of sections Criminal Law and Human Rights Law are discussed.

2.1.4 Other Legal Themes

Law as an academic discipline contains other themes outside the Private and Public Law dichotomy, and two of these have relevance in the thesis. However, Criminal Law and Human Rights Law can also be considered Public Law, but they are kept separate for the sake of heuristics, because they present drastically different problems in the intersection of law and cybersecurity in this thesis, and for Criminal Law, is only used in a limited manner. Criminal law only applies after the adversarial failure has occurred, and only with sufficient evidence, while Human Rights Law too

[125] See https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en, last accessed 11 December 2024.

[126] Regulation (EC) No 853/2004 of the European Parliament and of the Council of 29 April 2004 laying down specific hygiene rules for on the hygiene of foodstuffs [2004] OJ L139.

[127] Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters [2012] OJ L 351/1.

[128] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU OJ L117/176.

require extensive litigation before it can have any effect. This is quite different from the actions that are possible within Administrative Law, and the open procedures for Private Law litigation.

Criminal Law

Criminal Law can be situated within Public Law or outside of it.[129] In this situation, keeping it outside is more adequate, as it is only sparingly mentioned and used in the thesis, and because its origin can be viewed separate from Public Law. This is framed by the origin of legal sources and definitions. If "Public Law" refers to everything from constitution and down, Criminal Law is included, but if "Public Law" refers to Administrative Law, Criminal Law can be considered separate. It too stands as one of the oldest branches of law.[130]

Criminal Law is well known for existing mostly *ex post*,[131] meaning used after the crime has occurred, and occasionally *ex ante*, before the occurrence of a crime with deterrence and prevention.[132] Criminal Law can therefore be seen as deterrence or consequence based, and in a cybersecurity context, only applies to crimes where the adversarial attack and subsequent failure can be proven to have caused or assisted in the crime. Criminal liability for inadequate defences by manufacturers or users of systems does, at the time of writing, not exist in any jurisdiction in a literal sense. There may be situations where the inadequate defence can

[129]John Henry Merrymant, "The Public Law-Private Law Distinction in European and American Law" (1968) 17(1) Journal of Public Law 3.

[130]Donald L Magnetti, "Oath-functions and the oath process in the civil and criminal law of the ancient near east" (1979) 5(1) Brooklyn Journal of International Law 1.

[131]Peter Westen, "Two Rules of Legality in Criminal Law" (2006) 26(3) Law and Philosophy 229 ⟨http://link.springer.com/10.1007/s10982-006-0007-7⟩; PaulH Robinson, "Functional Analysis of Criminal Law" (1993) 88(3) Northwestern University Law Review.

[132]"The Role of Deterrence in the Formulation of Criminal Law Rules: At Its Worst When Doing Its Best" (2003) 91(5) Georgetown Law Journal (Thom Brooks ed 949 ⟨https://www.taylorfrancis.com/books/9781351944991⟩.

be argued to have indirectly caused financial damage, physical injury or death, but these are few and far between,[133] but if the poor defences lead to damage to infrastructure, some countries like Slovakia do have criminal liability for those who manage cybersecurity, albeit it is defined in a quite vague manner.[134]

This thesis does not use the term cybercrime,[135] or discuss any of the themes surrounding this, as many types of cybercrimes do not involve any cybersecurity elements, such as cyber stalking,[136] cyber bullying[137] and so on. But, these are important developing areas within Criminal Law, and should be considered if social engineering[138] or other cybersecurity related attack techniques are used, as is often seen in phishing.[139] This does not make the field of cybercrime less closely tied to cybersecurity, but to cover the whole area would include considerations into sciences which are not part of the scope of this thesis, such as anthropology and criminology. This, combined with a large part of cybercrime not directly interacting with cybersecurity, makes it less relevant for this thesis.

The behaviour of each developer of cybersecurity, as well as companies, is paramount, but there is surprisingly little research on the role which

[133] Examples could be James Christie, "The post office horizon it scandal and the presumption of the dependability of computer evidence" (2020) 17(March) Digital Evidence and Electronic Signature Law Review 49

[134] Miroslav Kelemen, Stanislav Szabo, and Iveta Vajdová, "Cybersecurity in the Context of Criminal Law Protection of the State Security and Sectors of Critical Infrastructure" [2018] Challenges to national defence in contemporary geopolitical situation 100 ⟨https://journals.lka.lt/doi/10.47459/cndcgs.2018.14⟩.

[135] Alisdair A Gillespie, *Cybercrime: Key issues and debates* (Routledge 2015).

[136] Alok Mishra and Deepti Mishra, "Cyber Stalking: A Challenge for Web Security" in *Examining the Concepts, Issues, and Implications of Internet Trolling* (2013).

[137] Joyce Kerstens and Sander Veenstra, "Cyber Bullying In The Netherlands: A Criminological Perspective" [2016] (Publisher: Zenodo) ⟨https://zenodo.org/record/55055⟩ accessed 20 February 2023.

[138] Jan-Willem Bullée and Marianne Junger, "Social Engineering" in Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (Springer International Publishing 2020) ⟨http://link.springer.com/10.1007/978-3-319-78440-3_38⟩.

[139] Bartlomiej Hanus, Yu Andy Wu, and James Parrish, "Phish Me, Phish Me Not" (2022) 62(3) Journal of Computer Information Systems 516 ⟨https://www.tandfonline.com/doi/full/10.1080/08874417.2020.1858730⟩ accessed 16 February 2023.

criminal law and liability could play in contributing to better security or otherwise control them,[140] which is a partial focus of Chapter 5, as there are few consequences for those leaving the massive supply chains of the world highly vulnerable to very simple cyberattacks.

The thesis also briefly considers the Online Safety Act[141] from the UK, and the proposed Child Sexual Abuse Regulation[142] in Chapter 4.

Human Rights Law

Human Rights Law is considered a subset of both International and Constitutional Law and could therefore also have been included as a part of Public Law section above. This thesis includes some Human Rights Law, and not International or Constitutional Law. Human Rights can be considered a relatively recent invention,[143] but it has a strong connection to the ideas of Natural Law, and many prominent non-lawyers have intensely discussed these merits before its inception in the twentieth century.[144] Rights must be protected and exercised legally, otherwise they are merely thoughts about aspects of human life, which is why the term Human Rights Law, and not just Human Rights, is what is used in this thesis.

There is a great difference between the rights given nationally, and those given within International Law,[145] but there exists a middle ground with

[140]For other angles on this, see Kelemen, Szabo, and Vajdová (n 134).

[141]https://bills.parliament.uk/bills/3137, last accessed 11 December 2024.

[142]European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (2022).

[143]This claim is contested, see Jack Donnelly, "Human Rights as Natural Rights" (1982) 4(3) Human Rights Quarterly 391, where Human Rights could be argued to go back to the ideas of *Locke*, from Natural Rights, making the concept much older. On the contrary, see Yves Dezalay and Bryant Garth, "From the Cold War to Kosovo: The Rise and Renewal of the Field of International Human Rights" (2006) 2(1) Annual Review of Law and Social Science 231 ⟨https://www.annualreviews.org/doi/10.1146/annurev.lawsocsci.2.032406.145708⟩.

[144]Carl Wellman, "The Universality and Justification of Human Rights" (2011) 30(3) Criminal Justice Ethics 288. A further discussion of the connection of Natural Rights and Human Rights could be taken but is outside the scope of this thesis.

[145]The specific difference lies in the first, national rights, being given on concrete grounds, while the latter represent more idealised concepts, but do not confer anything

the European Convention for Human Rights.[146] This convention by the Council of Europe[147] has effects on Human Rights in most states where it is implemented.

The main reason for this is implementation. Rights only exist if they can be realised through proper implementation or realisation, and if not possible to assert through these tools, the rights only exist on paper or in the treaties, conventions, and constitutions.

In EU member states, it was further enforced through the Charter on Fundamental Rights,[148] which was created to be similar to the Convention[149] and be means to guarantee its rights within EU Law. However, implementation of the Convention to members of the Council of Europe outside of the EU remains unsure.[150]

Cybersecurity and Human Rights are analysed together by some authors,[151] but otherwise remain a niche field.

In the context of this thesis, a discussion on Human Rights Law can be

unless implemented nationally in the first place.

[146]Council of Europe, European Convention on Human Rights ⟨https://www.echr.coe.int/Documents/Convention%7B%5C_%7DENG.pdf⟩.

[147]The Council of Europe is an international organisation formed after the Second World War, and has no relationship to the European Union. Its purpose is peace building and Human Rights, and by writing and getting signatures, ratifications, and implementations of the Convention, it has a direct effect on Human Rights Law of its members.

[148]Samantha Besson, "European human rights, supranational judicial review and democracy : thinking outside the judicial box" in *Human rights protection in the European legal order : The interaction between the European and the national courts* (Intersentia 2011).

[149]It most famously diverged by adding a right to Data Privacy, in Art 9, inspired by the earlier mentioned Convention 108 of the European Council.

[150]See, e.g., Anthony Cullen and Steven Wheatley, "The Human Rights of Individuals in De Facto Regimes under the European Convention on Human Rights" (2013) Human Rights Law Review(13) 4.

[151]Scott Shackelford, "Human Rights and Cybersecurity Due Diligence: A Comparative Study" [2017] (50.4) University of Michigan Journal of Law Reform 859 ⟨https://repository.law.umich.edu/mjlr/vol50/iss4/1/⟩; Ronald J Deibert, "Toward a Human-Centric Approach to Cybersecurity" (2018) 32(4) Ethics & International Affairs 411 ⟨https://www.cambridge.org/core/product/identifier/S0892679418000618/type/journal_article⟩; Pavlina Pavlova, "Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups" (2020) 4(11/2020) Peace Human Rights Governance 391 ⟨https://doi.org/10.14658/pupj-phrg-2020-3-4⟩; Nezir Akyesilmen, "CYBERSECURITY AND HUMAN RIGHTS: NEED FOR A PARADIGM SHIFT?" (2016) 1(1) Cyberpolitik Journal 25.

found in Chapter 4, where they are analysed through case law from the European Court of Human Rights. This brings a concrete discussion of rights to the technical specifications of measures which involve cybersecurity.

Next is the technical background, starting out with cybersecurity understood broadly.

2.2 Cybersecurity

Encryption has existed ever since the idea of secrecy in communications,[152] and the general principles and concepts of safety and security likely came with the development of architecture or construction of buildings in early societies. This is far older than the rest of cybersecurity, which was envisioned and shaped in the last and current century. Starting this section out with some considerations from non-digital security is therefore adequate, and only then continuing into the background and development of cybersecurity, both in computer science and engineering.

2.2.1 Non-digital Security

Security as a concept has existed at least since the idea of secrecy of communication,[153] but likely before in the management of protection of wares or goods as well. Orders given by superiors on the battlefield, or during the

[152] Kerckhoffs (n 2).

[153] John F Dooley, "Cryptology Before 1500 – A Bit of Magic" in *History of Cryptography and Cryptanalysis* (Series Title: History of Computing, Springer International Publishing 2018) ⟨http://link.springer.com/10.1007/978-3-319-90443-6_2⟩; Christopher H Walker, "Document Security in the Ancient World" in *Encyclopedia of Information Ethics and Security* (2007); Temba T Rugwiji, "Rereading Narratives of Safety and Security in Ancient Israel from a Pastoral Perspective" (2018) 27(1) Journal for Semitics ⟨https://unisapressjournals.co.za/index.php/JSEM/article/view/3559⟩. For a perspective on ancient encryption systems and its potential outside of the Western World, see Aman Kishore Agarwal and Deepesh Kumar Srivastava, "Ancient Katapayadi System Sanskrit Encryption Technique Unified" (IEEE July 2014) ⟨http://ieeexplore.ieee.org/document/6884947/⟩.

trading of wares and goods, were to be kept secret or secure, which even back then could be done through simple means of encryption,[154] physical security,[155] or through layers of security detail protecting the courier or the deliverable. Documented ciphers for the secrecy if messages existed at least as early as 50 BC, with the best known example being the one used by Julius Caesar.[156]

A distinction between security, in the form of protection of the confidentiality of the messages or wares, and safety through the integrity of staff, and availability of the messages and wares can already be glimpsed here, and these continue into cybersecurity today through the *CIA triad*.[157] This is defined as Confidentiality, Integrity and Availability. These characteristics are applied to the system generally, attacks, and failures, and they are universally shared and agreed on in security.

A specific physical type of security, locks and lockpicking, have long been used as an example and showcase later in cybersecurity.[158] These concepts are likely as old as civilization, but unlike older types of encryption and security details, locks are increasingly developed and changed,[159] alongside modern cybersecurity. This also mirrors the attackers versus defenders dichotomy closely, which is still the centre of cybersecurity proper.

---

[154]John F Dooley, *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms* (History of Computing, Springer International Publishing 2018) ⟨http://link.springer.com/10.1007/978-3-319-90443-6⟩.

[155]Jana Dambrogio and others, "Unlocking history through automated virtual unfolding of sealed documents imaged by X-ray microtomography" (2021) 12(1) Nature Communications 1184 ⟨https://www.nature.com/articles/s41467-021-21326-w⟩.

[156]
Dooley, "Cryptology Before 1500 – A Bit of Magic" (n 153) 14.

[157]Kosseff, "Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System" (n 107) 5.

[158]Michael Weiner and others, "Security analysis of a widely deployed locking system" [2013] Proceedings of the ACM Conference on Computer and Communications Security 929 (ISBN: 9781450324779).

[159]Matt Blaze and T Labs, "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks" [2002] 12.

2.2.2 Development of Cybersecurity

As the complexity of the systems increased, so did the needs and specifications of cybersecurity. While this is true now, due to the concept of physical cybersecurity and access control, there has never been a time where cybersecurity was not involved in digital systems. As long as computational power has been around, so has physical limitation of who can access and use the systems, which constitutes the oldest type of cybersecurity.[160] In the literature, there has been some thoughts related to periods where researchers and many others freely shared and used their systems,[161] but even during this era adversaries and defences existed.

Cybersecurity saw a large transition, when defences were not just needed by states and large corporations, but also in the homes of individuals with the creation of digital systems for home use. Access control, internal defences, and increased complexity due to the advent of the internet only exponentially increased the effort needed to keep devices safe.

IoT, robots, and cyberphysical systems are some of newer branches on the tree, while quantum computing and quantum encryption may significantly change cybersecurity. Although the latter may come with pitfalls, including being vulnerable to conventional attacks,[162] and has no full guarantee of ever happening, it is still worth discussing and analysing ahead of time.

Since cybersecurity is also practised within engineering, the background for this specific connection must be taken into consideration. In many sit-

[160] Arunesh Sinha and others, "From physical security to cybersecurity" [2015] Journal of Cybersecurity tyv007 ⟨https://academic.oup.com/cybersecurity/article-lookup/doi/10.1093/cybsec/tyv007⟩.

[161] Willis H Ware, "Security and privacy in computer systems" [1967] Proceedings of the April 18-20, 1967, Spring Joint Computer Conference 4.

[162] AP Pljonkin, "Vulnerability of the Synchronization Process in the Quantum Key Distribution System" (2019) 9(1) International Journal of Cloud Applications and Computing; Aydin Aysu and others, "Horizontal side-channel vulnerabilities of post-quantum key exchange protocols" (IEEE April 2018) ⟨https://ieeexplore.ieee.org/document/8383894/⟩.

uations, there may be no discernible difference between computer science and cybersecurity related engineering, but the devil lies in the detail. General computer science, in its theoretical form and through development of novel models and defences create the basis of cybersecurity, while engineering creates the practical implementation of the solutions, which is reflected in the difference in the major methods adopted within each domain.

2.2.3 Engineering as such

Engineering as a discipline can be discussed as a whole or divided into subdivisions for the sake of heuristics and concept. In this thesis, the general idea of it is applied, and methodological considerations for this can be found later in this chapter.

2.2.4 Engineering Terms and Concepts

Some of the core principles used in the thesis from engineering are listed here. These are all applied across the thesis and carry the same meaning unless otherwise specified in the chapters.

Safety

The term can be defined in a variety of ways, one of which is "Safety is freedom from accidents or losses".[163] It is therefore both a goal and a practice to reach safety. Historically, it has likely existed as long as dangerous technology has been in use, due to the obvious nature of wanting to save human lives during construction.[164]

[163]Nancy G Leveson, *Safeware: System Safety and Computers* (1., Addison-Wesley Publishing Company, Inc 1995) 181.

[164]This is regardless of the view on humans at the time, as dead individuals, slaves or not, are not more productive than those that are alive. Exceptions to this are found in "evil law", such as the Gulags of the USSR, Anna Lukina, "Making Sense of Evil Law" [2022]

It is practically shaped by the process to reach the goal, which means that good practice and successful designs and ideas rule, but failures contribute greatly to the knowledge as well. The latter is also the case for security and indeed for much of engineering more generally.

In a cybersecurity context, safety applies when analysing accidents or losses stemming from adversaries or consequences of adversarial failures, but not from adversarial failures in general. The application of safety is therefore specific in this thesis, but plays a significant role in designing robotics, IoT, and cyberphysical systems, to limit the amount of damage which is caused by accidents, be it physical or financial.

Safety is applied in most chapters in various forms.

The term safety-critical is mentioned once below and refers to a system being critical to the safety of something else, be it society, supply chains, or else. It is widely used in cybersecurity, but originally stems from safety, but should be understood literally and not in any expanded or otherwise different sense.

Security and Cybersecurity

Security as a concept is much older than safety and has been negatively defined through Criminal Law ever since its inception. In the context of the Code of Hammurabi, its punishments and rules singled out unwanted behaviour and the prevention of murder and theft.[165] Crimes occurring could then be characterised as security failures on a societal level, and as such, cybersecurity can be defined in an equivalent manner:

Cybersecurity is freedom from adversarial failures, which affect digital systems. The specification of the adversarial failures specifically affecting

SSRN Electronic Journal ⟨https://www.ssrn.com/abstract=4180729⟩. Other exceptions would be after the Industrial Revolution, where workers were assumed to have accepted the dangerous risks, Leveson (n 163) 129-130.

[165] Hammurabi's Code of Laws (n 6).

digital systems is necessary, because physical cybersecurity can be caused by non-digital means.

Cybersecurity and security are therefore synonyms, though the latter spans everything from preventing robberies to the prevention of war, while cybersecurity only exerts itself through digital systems, with the important exceptions of physical cybersecurity. The old principles from security will apply here, many of the same techniques which keeps a bank vault safe will work on building or housing important servers. One notable difference is side-channel attacks and adversarial techniques which go through walls or rely on measurements which cannot be prevented, but some physical defences exist for these too.

Like safety, the practical implementation of security consists of the means to prevent it, but unlike safety, this is against adversaries at all times.[166] There are therefore different considerations, such as the behaviour of the attacker, their capabilities within the system and more. Instead of being an attempt to prevent the system or its user from causing accidents, it is instead an open fight between attackers and defenders in every single system, at any given point.

Cybersecurity is done through many types of research, including empirical,[167] but reconstructing the tools of adversaries and predicting vulnerabilities (with proper disclosure) remains the classic in the form of attack papers.[168] Nowadays, attack papers include novel or otherwise clear de-

[166] See Chapter 2 in Anderson (n 3).

[167] Hatma Suryotrisongko and Yasuo Musashi, "Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective" (IEEE November 2019); Abdulmajeed Alahmari and Bob Duncan, "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence" (IEEE June 2020) ⟨https://ieeexplore.ieee.org/document/9139638/⟩.

[168] There are many examples, a few relevant to this thesis are Christos Xenofontos and others, "Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies" (2022) 9(1) IEEE Internet of Things Journal 199 ⟨https://ieeexplore.ieee.org/document/9430606/⟩ accessed 28 July 2023; Asanka P Sayakkara and Nhien An Le-Khac, "Forensic insights from smartphones through electromagnetic side-channel analysis" (2021) 9 IEEE Access 13237; Sara Kaviani, Ki Jin Han, and Insoo Sohn, "Adver-

fences that can defeat the techniques that are proven earlier. Otherwise, this remains the core in defence papers, where the adequate technique, approach, or means to mitigate or prevent attacks are shown.[169] Both of these traditions go as far back as locksmithing research, where this dichotomy also existed.[170]

Risk in Cybersecurity

While cybersecurity in general creates the foundational understanding of *how* adversarial failures can occur, risk explains *how often*. A suitable definition for risk is *"the likelihood of a failure occurring"*.

In some situations, the severity of the risk is considered as well, but if we limit it to purely managing and comprehending the estimated or measured statistics behind it, a problem is encountered. While we seek knowledge of when something can occur, likelihood itself cannot answer this.[171] If done without any kind of empirical analysis backing it, it is simply an estimate, deriving no notion of whether it will actually happen, and is incapable of answering the questions given.[172] If the likelihood does contain historical

sarial Attacks and Defences on AI in Medical Imaging Informatics: A Survey" [2022] Expert Systems With Applications 116815 (Publisher: Elsevier Ltd.) ⟨https://doi.org/10.1016/j.eswa.2022.116815⟩; Hui Lin and others, "Safety-Critical Cyber-Physical Attacks : Analysis, Detection, and Mitigation" [2016] 82 (ISBN: 9781450342773).

[169]Chunxiao Li, Anand Raghunathan, and Niraj K Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system" [2011] 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2011 150 (ISBN: 9781612846972 Publisher: IEEE); Daniel Halperin and others, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses" [2008] Proceedings - IEEE Symposium on Security and Privacy 129 (ISBN: 9780769531687); Xueluan Gong and others, "Model Extraction Attacks and Defenses on Cloud-Based Machine Learning Models" (2020) 58(12) IEEE Communications Magazine 83 ⟨https://ieeexplore.ieee.org/document/9311938/⟩; Mehran Mozaffari-Kermani and others, "Systematic Poisoning Attacks on and Defenses for Machine Learning in Healthcare" (2015) 19(6) IEEE Journal of Biomedical and Health Informatics 1893 ⟨http://ieeexplore.ieee.org/document/6868201/⟩.

[170]Which continues still, see e.g., Weiner and others (n 158); Blaze and Labs (n 159).

[171]Nau (n 54).

[172]For other perspectives on this, see Jan Folkmann Wright, "Risk management; a behavioural perspective" (2018) 21(6) Journal of Risk Research 710 (Publisher: Routledge) ⟨http://dx.doi.org/10.1080/13669877.2016.1235605⟩.

data, it may be accurate in a safety setting[173], but because adversaries are human, modelling this onto any given system becomes difficult, and certainty is impossible.

This explains why much cybersecurity research focuses on the possibility, and not on the likelihood or probability. When the systems, which the risk is measured from, function continuously, risks which are estimated to be low happen more frequently. The latter is the problem with viewing low percentage risks as "uncommon", as it depends on the system.

2.3 Methodology

The following section explains the methods which are applied in the thesis. The chosen methods amount to doctrinal and comparative legal methods, and theoretical computer scientific method for cybersecurity, with additional usage of safety engineering method to account for safety aspects of the thesis.

2.3.1 Methods in Law

In this section, an overview of doctrinal and comparative legal method as used in this thesis is given.

Doctrinal Method

Applied, practiced, and academic law in Common Law countries, like the US and the UK, have historically not always considered specifically which method they study law with and why, but deferred to a bare minimum and

[173] Safety engineering is based on the notion that this past data can be used to design safer systems, but even within closed circuits, accidents and unpredictable hazards can occur with systems that run for long or often, which can become an occurrence that happens more than may be thought. This creates the basis of the criticism purely within safety, that is, likelihood still does not answer or otherwise solve the question of *how often* even here.

logical constructs which match the institutions and the legal system they work in.[174] The lack of definitions come from the practice of law, where identification of methods is unnecessary if they present no academic or practical problems. This is usually referred to as "doctrinal method", and can be defined as:

Research which provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments.[175]

Outside of Common Law, this is not the case, and established directions and reverence of specific theoretical approaches have long dominated scholarly discussions of law.[176]

In the context of this thesis, doctrinal legal method consists of first finding *de lege lata* (law it is), and argue for *de lege ferenda* (law as it should be),[177] the latter either continuing from how *de lege lata* currently looks, fulfils the spirit and purpose of it, or the opposite, *de lege ferenda* needing to be completely different to fulfil requirements seen in other legislation or elsewhere in society. This is the main theme of the thesis, that requirements outside of law, here cybersecurity, may implore *de lege ferenda* to be significantly different than *de lege lata*.

Chapter 3, 4, and 5 provide suggestions for improvements for existing law,

---

174

Terry Hutchinson and Nigel Duncan, "Defining and Describing What We Do: Doctrinal Legal Research" (2012) 17(1) Deakin Law Review 83 ⟨https://ojs.deakin.edu.au/index.php/dlr/article/view/70⟩.

175

Specific wording is from the Australian Pearce Committee, but it captures exactly what Doctrinal Method really is, ibid 101.

176 This has been ongoing since the early nineteenth century in Denmark, through the methodological shift instigated by A. C. Ørsted, Ross (n 51) 154. For additional perspectives in English, see Ulf Bernitz, "What is Scandinavian Law?" (2007) 50(1) Scandinavian studies in law; Henry Ussing, "The Scandinavian Law of Torts: Impact of Insurance on Tort Law" (1952) 1(4) The American Journal of Comparative Law 359 ⟨https://academic.oup.com/ajcl/article-lookup/doi/10.2307/837349⟩.

177 This short approach is exactly as the Pearce Committee defined earlier, but is explicit in including *de lege ferenda*.

taking characteristics of reform-oriented research. This does not significantly diverge from doctrinal legal method as it is used in Scandinavian Law, and Common Law scholars have also shifted in this direction in the twentieth century,[178] emphasising the character and amount of *de lege ferenda* analysis.

Moving on to the second type of legal research method used in this thesis is now necessary, which is the methodology behind comparing different legal systems, Comparative Law.

Comparative Legal Method

Law exists in jurisdictions in individual countries, this entails understanding each legal system and being able to compare them.[179] The exact methods and characteristics are still heavily debated,[180] but the approach, distinction and understanding of Comparative Law used here, is the one given by Zweigert and Kötz.[181] Firstly, a research question must be posed,[182] while attempting to understand each legal system and their differences. Secondly, the equivalent rules and concepts in each legal system must be identified,[183] and whether or not these should be analysed on their own merits (individually) or viewed as similar to the structures in other sys-

[178]Terry Hutchinson, "The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law" [2016] Erasmus Law Review (Sanne Taekema ed ⟨http://www.elevenjournals.com/doi/10.5553/ELR.000055⟩; Hutchinson and Duncan (n 174).

[179]Comparative Law here refers only to comparing the legal systems of national states.

[180]Ralf Michaels, "Comparative Law by Numbers? Legal Origins Thesis, Doing Business Reports, and the Silence of Traditional Comparative Law" (2009) 57(4) American Journal of Comparative Law 765 ⟨https://academic.oup.com/ajcl/article-lookup/doi/10.5131/ajcl.2008.0022⟩; Oliver Brand, "Conceptual Comparisons: Towards a Coherent Methodology of Comparative Legal Studies" (2007) 32(2) Brooklyn Journal of International Law; Günter Frankenberg, "Critical Comparisons: Re-thinking Comparative Law" in *Legal Theory and the Legal Academy* (Taylor & Francis 2010); Sue Farran and Esin Orlcfl, "The Continuing Relevance of Comparative Law and Comparative Legal Studies" (2019) 6(2) Journal of International and Comparative Law; Levmore (n 74); Comparative Law and Interdisciplinarity (n 1).

[181]Zweigert and Kötz (n 68).

[182]ibid 34.

[183]ibid 36.

tems. Thirdly, the country studied can be put into the context of Common Law or Civil Law, or any other specialised legal family or group.[184] Fourthly, the comparison is not the end goal or the findings, analysing the differences in a total context and to answer other questions should be what is desirable.[185] Fifth, a system of the differences or similarities must be build, even if only conceptually, to facilitate the comparison.[186] Sixthly, a critical evaluation must be created,[187] which in the context of this thesis always rests on the research question posed by the entire chapter itself.

This can be summarised to *respect and understand selected legal systems, identify relevant and/or equivalent rules, place countries in relevant families or groups, remember that comparison is not the goal in itself, systematise findings and critically evaluate*. To this, this thesis' use of Comparative Method is aimed at showing alternative solutions to specific problems and does not constitute the primary legal methodology.

Comparative legal method is used in Chapter 5 to illustrate different implementations of EU Law, and how each jurisdiction may potentially sanction providers of cybersecurity. The strength of this method allows for an overview of the concepts in each system, but a weakness is how similar rules in each legal system can be different in practice, which are so-called false equivalences. These remain a common weakness of comparative legal method.

In the next section, the methodology from cybersecurity used in the thesis is discussed.

[184]Zweigert and Kötz (n 68) 42.
[185]ibid 43.
[186]ibid 44.
[187]ibid 47.

2.3.2 Applied Methodology in Cybersecurity

While cybersecurity is a broad, branched, and wide-spanning field, it is also a sub-field within computer science, which means general methodology and ontology from computer science applies. In this thesis, we make use of two distinct directions in the form of Theoretical Computer Scientific Method and Theoretical Engineering Methods, the former as cybersecurity within computer science, and the latter as cybersecurity and safety engineering. Engineering is unique, in that it creates sub-fields within other sciences rather easily, exemplified by development papers.[188] Essentially, these new fields occur when the engineering tools of modelling, development of frameworks, and focus on pragmatic usage and perspectives are applied to them.

Cybersecurity in Computer Science

Methodology within computer science in general either employs generic scientific method, or more specialised theoretical and empirical computer scientific methods.[189] The distinction between deduction and induction is very clear, as formal verification and proofs consist of deductive logic, while empirically proving or otherwise justifying the technology or development is done through inductive logic.

Cybersecurity as a field is also extremely diversified, and each sub-field employs unique approaches and methods, as can be seen in the difference

[188] Kathleen M Carley, "Computational organizational science and organizational engineering" (2002) 10(5-7) Simulation Modelling Practice and Theory 253 ⟨https://linkinghub.elsevier.com/retrieve/pii/S1569190X02001193⟩; William J Mitsch and Sven E Jørgensen, "Ecological engineering: A field whose time has come" (2003) 20(5) Ecological Engineering 363 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0925857403000600⟩.

[189] Gordana Dodig-Crnkovic, "Scientific Methods in Computer Science" [2002] Proceedings of the Conference for the Promotion of Research in IT at New Universities and at University Colleges in Sweden, Skövde, Suecia 7; Petro Luzan and others, "The Methodology for Assessment of Engineering Students Outcomes" (IEEE September 2021) ⟨https://ieeexplore.ieee.org/document/9598666/⟩.

between the study of protocols versus the study of physical cybersecurity. The former primarily consists of deductive proofs, or simulations through game theory or other rather deductive means to argue for efficiency and so on, and the inductive arguments consist of empirically gathering evidence through testing of these protocols. Physical cybersecurity has no deductive proofs or arguments, and primarily shows security through inductive arguments from testing, showcasing attacks and defences, and even employing psychological methodologies to prove how humans make mistakes and cause insecurity in a physical context.

In this thesis, deductive arguments from theoretical aspects of cybersecurity are primarily employed, and ideas based on inductive arguments derived from empirical studies from the issues which we discuss serve as the reflection of the current state of the research field and industry. The latter overlaps with the cybersecurity engineering aspects of the field.

The next short section explains the role of multidisciplinary and interdisciplinary methods.

2.3.3 Multidisciplinarity and Interdisciplinary Methods

This thesis makes use of both multidisciplinary, and partially, interdisciplinary methods. While the latter is not followed fully through, both types need clarification, which will be provided below.

There are a range of definitions and understandings of multidisciplinary methods,[190] but they all share the lack of union which interdisciplinary methods provides. Multidisciplinary studies make use of different disciplines, be it methodologically or through their understanding, but will not

[190] JT Dillon, "The Multidisciplinary Study of Questioning" (1982) 74(2) Journal of Educational Psychology 147; Dhruv Grewal and others, "The future of technology and marketing: a multidisciplinary perspective" (2020) 48(1) Journal of the Academy of Marketing Science 1 ⟨http://link.springer.com/10.1007/s11747-019-00711-4⟩ accessed 17 December 2023; Peter Van den Besselaar and Heimeriks Gaston, "Disciplinary, multidisciplinary, interdisciplinary: Concepts and indicators" [2001] ISSI.

necessarily combine it all in its conclusion.[191]

The reason this thesis does not only make use of this, is that for all chapters, there will be conclusions which make use of both law and cybersecurity, and even safety, meaning that multidisciplinary method cannot be used by itself.

Interdisciplinary methods are no longer uncommon and can be found in combination with law and computer science in a myriad of ways, including through safety,[192] medicine,[193] engineering[194] and much more.[195] New scientific fields are born from the combination of methods from two or several sciences, this can be seen with Computational Law,[196] but computer science was originally a combination of at least math and physics in its current form.[197]

This thesis combines methodologies from law and cybersecurity, which in practice means applying doctrinal and comparative legal method together

[191] Van den Besselaar and Gaston (n 190) 2.

[192] Simon Burton and others, "Mind the gaps: Assuring the safety of autonomous systems from an engineering, ethical, and legal perspective" (2020) 279 Artificial Intelligence 103201 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0004370219301109⟩. For an example of an interdisciplinary paper without computer science, see Anne Marie Lofaso, "Approaching Coal Mine Safety from a Comparative Law and Interdisciplinary Perspective" (2008) 111(1) West Virginia Law Review.

[193] Jessica Jue, Neal A Shah, and Tim Ken Mackey, "An Interdisciplinary Review of Surgical Data Recording Technology Features and Legal Considerations" (2020) 27(2) Surgical Innovation 220 ⟨http://journals.sagepub.com/doi/10.1177/1553350619891379⟩.

[194] Burton and others (n 192).

[195] Examples could include Johanna Jacob, Michelle Peters, and TAndrew Yang, "Interdisciplinary Cybersecurity: Rethinking the Approach and the Process" in Kim-Kwang Raymond Choo, Thomas H Morris, and Gilbert L Peterson (eds), *National Cyber Summit (NCS) Research Track* (Series Title: Advances in Intelligent Systems and Computing, Springer International Publishing 2020) vol 1055 ⟨http://link.springer.com/10.1007/978-3-030-31239-8_6⟩; Migle Laukyte, "An Interdisciplinary Approach to Multi-agent Systems: Bridging the Gap between Law and Computer Science" (2013) 22(1) Informatica e diritto; Thomas C King and others, "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions" (2020) 26(1) Science and Engineering Ethics 89 ⟨http://link.springer.com/10.1007/s11948-018-00081-0⟩; Katharina Bräunlich and others, "Linking loose ends: An interdisciplinary privacy and communication model" (2020) 23(6) New Media & Society.

[196] Burkhard Schafer, *Legal Tech and Computational Legal Theory* (Publication Title: Law and Technology in a Global Digital Society, 2022).

[197] Dodig-Crnkovic (n 189).

with computer scientific and engineering methods.[198] Law will by its very nature allow all types of evidence, as seen through how it is practiced in courts and elsewhere, usually as "facts" or expert witnesses, but using interdisciplinary methods allow the analysis to dive deeper. This is done by attempting to *genuinely understand the technical aspects which would otherwise be perceived with considerable distance*. The idea is to not dismiss or leave the otherwise technical understandings, specifications, or information to the expert witnesses or others who summarise it for litigation, instead making sure that the details are understood just as well as the legal rules. In this sense, the interdisciplinary approach allows the user to critique and understand non-law elements fully and implement all relevant considerations directly into the analysis.

While there are other authors who have made similar interdisciplinary choices akin to this thesis,[199] none have included both cybersecurity and safety engineering, and none have individually worked with both methodologies as is done here. *Jacob et al.* only narrowly define relevant areas which they believe law should interact with,[200] while not engaging further into the reality which cybersecurity brings, which is that it applies to every area where adversarial failures can occur. *Laukyte* develops novel frameworks and interdisciplinary concepts that are similar what has been done in this thesis, but outside of both cybersecurity and safety.[201]

In the next section, a methodological overview of each chapter is given for the sake of clarity.

[198] See this overview for where we may be in an interdisciplinary sense regarding cybersecurity, in Suryotrisongko and Musashi (n 167).

[199] Examples could be Suryotrisongko and Musashi (n 167); Jacob, Peters, and Yang (n 195); Laukyte (n 195).

[200] Jacob, Peters, and Yang (n 195) 66.

[201] Laukyte (n 195).

2.4 Applied Methods in the Chapters

Chapter 3 uses doctrinal legal method, as there is a considerable amount of classic analysis of *de lege lata*, law as it is, specifically within EU Law regarding Medical Devices, with some considerations on *de lege ferenda* and future law. It also involves national case law analysis, and since some parts are specifically regarding Danish cases, care has been taken to introduce the reader to the necessary foundations to understand it. The selected relevant cases, to explain gaps and exceptions, are all established case accepted in standard literature in Danish law. The reason these were picked is the use of soft law in the Danish legal system, in which Reimbursement Law specifically plays a key role.

In contrast, the other parts of Chapter 3 use of computer scientific method, with a strong safety focus, and creates multidisciplinary, and finally, interdisciplinary perspectives. This is done by first defining and describing a new way to understand adversarial attacks on surgical robots, to then discuss how new EU law is to be understood, and finally analyse Danish case law to answer various questions, while including the understanding of adversarial failures and weaknesses from cybersecurity.

In Chapter 4, doctrinal Legal Method and Theoretical Computer Scientific Method is used. By analysing the idea of a Client-side Scanning system, we go beyond law, but only in a multidisciplinary manner. Concerning the Human Rights Law, the chapter otherwise employs legal method through its case law analysis and conclusions on current and potential future law. The specific type of case law entails certain differences compared to the rest of the thesis, as the European Court of Human Rights is not national, containing dissimilar writing style and comprehension.

Chapter 5 is partially a straight *de lege feranda* analysis, as it primarily

concerns future law or law proposals, but it sprinkles in safety engineering principles, specifically the understanding and use of them, which means engineering methodology applies. However, interdisciplinary methodology is also a focus. The use of cybersecurity takes the role of evidence in a court case and serves as the arguments as to why and how, in this case Supply Chain Attacks, should be regulated, or how it is not covered by the implementation of EU Law in three jurisdictions.

3 | Adversarial Attacks in Medical Devices: Intention as a Measure Against Circumvention, and Cyberattacks in Litigation and Practice

3.1 Introduction

Software and applications play an ever-increasing role in healthcare and wellness. This is evident with the increased use of IoT devices, applications on smartphones for both professionals and consumers, and even more sophisticated software used by health professionals.[1]

As a recent example, several software-based solutions were proposed which would use mobility data from smartphones and wearables for disease surveillance. The European Commission issued a Recommendation *'on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications*

[1] Muhammad Mahtab Alam and others, "A survey on the roles of communication technologies in IoT-Based personalized healthcare applications" (2018) 6 IEEE Access 36611 (Publisher: IEEE).

and the use of anonymised mobility data.'[2] This was released after the WHO declared COVID-19 to be a pandemic on 11 March 2020.[3] Many organisations may have developed smartphone-based contact tracing methods without much consideration of the relevant regulatory landscape as a response to the pandemic. Data Protection and privacy concerns have been the focus when contract tracing methods were analysed,[4] but little regard has been paid so far to medical device regulatory frameworks. Among the many consequences of the virus, was the postponement of Regulation 2017/745 – the Medical Device Regulation (MDR),[5] which is also a primary focus of this chapter. It was postponed for a year and came into force on 26 May 2021. Before it was postponed, the European Commission issued the aforementioned Recommendation on COVID-19 technology and data. In its preamble 13, it states that the MDR, as well as the Medical Device Directive (MDD)[6] which was in force at the time, might apply to some of the mobile applications that could be used for diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease during the pandemic.[7] This could include self-diagnosis software, and the Commission directly asked for stakeholders to consider whether this type of software falls within the scope of the MDD and MDR.

[2]Commission Recommendation C(2020) 2296 (2020).

[3]https://twitter.com/WHO/status/1237777021742338049, last accessed 11 December 2024.

[4]See e.g., Linnet Taylor and others, *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020); Michael Dieter and others, "Pandemic platform governance: Mapping the global ecosystem of COVID-19 response apps" (2021) 10(3) Internet Policy Review ⟨https://policyreview.info/articles/analysis/pandemic-platform-governance-mapping-global-ecosystem-covid-19-response-apps⟩.

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

[6]Council Directive 93/42/EEC of 14 June 1993 concerning medical devices [1993] OJ L169/1.

[7]There exists a distinction between the MDD and directive 98/79 on in vitro medical devices, and vice versa with the MDR and its in vitro sibling. The in vitro directive and regulation are not used further in this chapter.

This presents a dilemma for lawmakers as to when this software, now much more widespread than previously, should be regulated in the same way as other medical equipment or medical devices (MD). Software can potentially harm or affect humans in the same way as physical equipment, which means it must be regulated with the same degree of rigour in cases where this is so. However, determining when software is a MD remains a tricky issue.[8] There is a range of reasons why it must be clear when software is and is not a MD, with the most urgent being the increased risks that software used as a MD pose.[9] Insecure software risks the mental and physical health of human beings. Security is a complex process that requires significant safety capital upfront during the design stage just like conventional MDs. Unlike conventional MDs, software as a MD also requires continuous updates to maintain security, which means a significant upfront cost as well as upfront cost, in addition to the ongoing cost of updates. Aside from economics, market incentives and a lack of regulation of software combine together to create an environment where security engineering is sadly not of a high standard.[10]

Before considering whether the existing legal requirements do take account of these challenges, current research on guidance derived from EU law for software is promising,[11] in the sense that the guidance does consider security failures,[12] because it is implied and accepted as a central

[8]In the field of MD regulation, the EU and the US are the two biggest players internationally. This makes analysis of their legislation relevant elsewhere, due to their effects on other jurisdictions.

[9]Kevin Fu and others, "Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things" [2020] Computing Community Consortium ⟨http://arxiv.org/abs/2008.00017⟩.

[10]Kevin Fu, "Trustworthy medical device software" (2011) vol 510 ⟨http://www.cs.ucsb.edu/%7B~%7Dsherwood/cs290/papers/fu.pdf⟩.

[11]Lisa Parker and others, "A health app developer's guide to law and policy: A multi-sector policy analysis" (2017) 17(1) BMC Medical Informatics and Decision Making 1 (ISBN: 1291101705 Publisher: BMC Medical Informatics and Decision Making).

[12]The issue with most of the guidance however, is that it is not legally binding, and in practice it is unclear the extent to which it is enforced, and as a result it may be left up to manufacturers to decide whether to follow it or not (if they are even aware of it in the

requirement for functioning when it comes to MD.[13]

Furthermore, the possible actions by regulators that can be directed to manufacturers are discussed in this chapter as well, as these will affect the manufacturer and maybe even later lawsuits against them. A specific example is surgical robots. Surgical robots are without a doubt considered medical devices, which means they are regulated by the European Medical Device Regulation (MDR),[14] since they fit the definition of "medical devices for human use" seen in Art 1(1). In the future, AI may even be able to partially or fully control surgical robots, which only make the role of security exponentially larger. Any discussion involving EU law means national law in each member state apply to them as well, because the use of surgical robots will always be covered by national healthcare rules and EU standards.[15]

Surgical robots enable unique approaches to treatment not possible before, with minimally invasive surgery being the primary technique. Two examples would be laparoscopy done by the da Vinci systems[16] and the Magellan system deployed for cardiac surgery.[17]

Surgical robots are widely used for a range of treatments,[18] for example

---

first place).

[13]See Chapter 1, 1, in Annex I in the Medical Device Regulation.

[14]Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L117/1. The MDR has applied fully since 26 May 2021.

[15]The European Commission is aware of this, see e.g., 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics', <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0064&from=en>, last accessed 11 December 2024. However, they do not go into a national legal system discussion.

[16]Operation by small incisions into abdomen or pelvis with the aid of a camera.

[17]Christos Bergeles and Guang Zhong Yang, "From passive tool holders to microsurgeons: Safer, smaller, smarter surgical robots" (2014) 61(5) IEEE Transactions on Biomedical Engineering 1565, 3.

[18]Chris Holder and others, "Robotics and law: Key legal and regulatory implications of the robotics age (part II of II)" (2016) 32(4) Computer Law and Security Review 557 (Publisher: Elsevier Ltd) ⟨http://dx.doi.org/10.1016/j.clsr.2016.05.011⟩, 388.

for hernia and intestinal cancer.[19]

Their increased usage is not without consequences, and criticisms of specific surgeries has started to occur, primarily aimed at the lack of empirical research that makes their efficiency likely.[20] This development has increased around the world, especially in the US and the EU.[21]

The surgeon and the patient are not the only relevant parties when it comes to surgical robots. Engineers, programmers, nurses, lawyers and a whole range of other staff are needed to design, produce, operate and maintain them,[22] and must handle and possibly mitigate accidents if they happen. Certain research on the perspective of manufactures and patients has been done in the area,[23] but it is still underdeveloped regarding the legal rights, liabilities, obligations and the choice of legal instruments and tools that are applied to surgical robots in general.

To legally discuss surgical robots, they, and the features of which they consist of must be categorised. For this chapter, considering them as cyberphysical systems (CPS)[24] is necessary, because they are robots that interface with the physical world,[25] with their tools being used directly on

[19]E.g., a da Vinci surgical robot from a small Danish hospital broke the record with 426 performed surgeries in 2019, and it is mainly used for the aforementioned treatments, see Henrik Dürr, "Vild statistik på sygehus: Robot står bag 1000 operationer" [2019] JydskeVestkysten ⟨https://jv.dk/aabenraa/vild-statistik-paa-sygehus-robot-staar-bag-1000-operationer⟩.

[20]Naila H Dhanani and others, "The Evidence Behind Robot-Assisted Abdominopelvic Surgery" (2021) 174(8) Annals of Internal Medicine 1100.

[21]See <https://www.medtechdive.com/news/intuitive-surgical-profit-up-on-strong-da-vinci-robot-sales/528257/>, last accessed 11 December 2024.

[22]This is especially important if they end up being partially or fully controlled by AI, which may have a negative social impact, see e.g., Emilio Gómez-González and others, "Artificial intelligence in medicine and healthcare: a review and classification of current and near-future applications and their ethical and social Impact" (_eprint: 2001.09778, 2020) ⟨http://arxiv.org/abs/2001.09778⟩ 5.

[23]See the note by Christopher Beglinger, "A Broken Theory : The Malfunction Theory of Strict Products Liability and the Need for a New Doctrine in the Field of Surgical Robotics" (2019) 104(2) Minnesota Law Review 1041, for a an example of an interdisciplinary approach with focus on liability in a US context.

[24]NSF, *Cyber-Physical Systems* (techspace rep, National Science Foundation 2014) 2.

[25]There is no doubt that many types of medication prescription systems, or those that monitor the health of the patient (but do nothing else), will be considered CPS even if they barely interface with the physical world.

the patient. Robots can be defined in variety of ways, but in this chapter its CPS nature is a focus.[26]

CPS has a tendency to erase the boundary between the physical and digital sphere, which is clearly seen in the many new ways which they can injure people or otherwise cause economical damage. The risk of injury or damage caused by the surgical robot, due to internal failure or deterioration, is called safety for both patients and anyone else surrounding the robot. If the surgical robot is compromised or otherwise is hit by a cyberattack, this is a security failure. Safety failures can lead to injuries but cyberattacks from individuals or organizations outside of the hospital are now able to cause safety failures as well.[27] Because surgical robots are CPS and are always connected to a network, security failures can cause safety failures. This means that cyberattacks on a surgical robot before or during operation can lead to physical injuries on the patient or the operator.

Expanding the understanding of what constitutes cyberattacks is necessary because it is only going to become more commonplace.[28] Any action that is intentional and seeks to induce failure, is considered a cyberattack.[29] The term "adversarial failure" and "adversarial attack" is used instead, as this allows us to consider non-adversarial failures alongside it, which may

[26]Other ways could be those proposed in Eduard Fosch-Villaronga and Christopher Millard, "Cloud robotics law and regulation: Challenges in the governance of complex and dynamic cyber–physical ecosystems" (2019) 119 Robotics and Autonomous Systems 77 (Publisher: Elsevier B.V.) ⟨https://doi.org/10.1016/j.robot.2019.06.003⟩, 13, which apply to robots in general and could be appropriate.

[27]Such as unwanted movement of tools inside the patient or the machine stopping entirely, see Homa Alemzadeh and others, "Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation" [2016] (395) Proceedings - 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2016 395 (ISBN: 9781467388917), 397.

[28]For an overarching EU perspective, see Sarah Backman, "Risk vs. threat-based cybersecurity: the case of the EU" (2023) 32(1) European Security 85 ⟨https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2069464⟩ accessed 24 May 2024.

[29]See working definition of all studies of adversarial behaviour/failure/attacks, e.g., Xiaohui Zeng and others, "Adversarial attacks beyond the image space" (2019) 2019-June Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition 4297 (ISBN: 9781728132938 _eprint: 1711.07183).

lead to the same kind of injuries as an adversarial failure.

Furthermore, there is a distinction between attack and failure, since the latter implies a failed state of the machine while the first can merely be an attempt to cause it (which may succeed).[30]

Security failures, whether caused by adversaries or non-adversarial failures, like accidents, can cause further harm when the software is essential for implantable and devices that otherwise affect the physical health of a human (such as pacemakers), and these are also known to have poor defences.[31] Using secure communication channels, robustness to malware and other harmful interference should be required, but there is no such explicit legal or practical requirement for software in general or MD software specifically, with no certification or authority investigating or inspecting this specific issue at the EU level.[32] There are also no requirements for ensuring software correctness, and that the software is built to a high standard.[33]

Regulation and law in general can be tools to mitigate and otherwise regulate risks. Both national and EU law are used on to the issues that adversarial attacks on surgical robots that lead to injuries present. This gives

[30]Within security research, failure states of systems like a surgical robot being controlled by an adversary, are different than a successful attack which then does not cause a subsequent failure. For an example of how the failure state is studied and compared to the adversarial attacks (here adversarial examples), see Richard Tomsett and others, "Why the Failure? How Adversarial Examples Can Provide Insights for Interpretable Machine Learning" [2018] 2018 21st International Conference on Information Fusion, FUSION 2018 838 (ISBN: 9780996452762).

[31]Carmen Camara, Pedro Peris-Lopez, and Juan E Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey" (2015) 55 Journal of Biomedical Informatics 272 (Publisher: Elsevier Inc.) ⟨http://dx.doi.org/10.1016/j.jbi.2015.04.007⟩.

[32]Maged N Kamel Boulos and others, "Mobile medical and health apps: state of the art, concerns, regulatory control and certification" (2014) 5(3) Online Journal of Public Health Informatics 1.

[33]Correctness here refers to e.g. correct clinical advice that resembles that given from a physician, or correct analysis of biometric data which fits what would be conducted in traditional MDs. See, e.g., Ma R Cantudo-Cuenca and others, "A better regulation is required in viral hepatitis smartphone applications" (2014) 38(2) Farmacia Hospitalaria 112; Daniel J Stevens and others, "Obesity surgery smartphone apps: A review" (2014) 24(1) Obesity Surgery 32.

us an in-depth perspective on when the attack is successful and someone has to cover the damages done to the patient,[34] and the obligations and liabilities incumbent to the manufacturers in the context of the MDR. This also constitutes the context which this chapter answers the two questions posed in the introduction.[35]

Surgical robots present unique security considerations, and this chapter will therefore include a framework for considering specific ways that a surgical robot can fail and potentially harm the patient. After the framework is introduced, it is tested in two different cases. Secondly, these CPS specific risks will be analysed from a legal perspective as well, since this will show whether existing systems are capable of handling and otherwise mitigating them, both concerning security (both before deployment and after) but also the legal aftermath when the injuries have occurred.[36]

The chapter therefore contains definitions in section 3.2, analysis and overview of the MDR in 3.3 with an emphasis on manufacturers and authorities, the framework for intention which expands the MDR in section 3.4, how this framework can be applied in 3.5, the case of Danish law and adversarial attacks on surgical robots in section 3.6, further comments on adversarial attacks in court and how they can be dealt with in section 3.7, future work in section 3.8, and finally the conclusion in section 3.9.

[34]The situation where the attacker is identified is not discussed in this chapter, since this would devolve into general criminal prosecution and the subsequent civil lawsuits.

[35]"How can this legal concept be understood in cybersecurity," and "how can these cybersecurity considerations be understood in law"?

[36]Whether legislation must updated as frequently as the technology regulates, is not the scope of this chapter, but it seems to be an open question regardless of the papers in the area, see e.g., Koops (n 17), Ohm (n 17), Reed (n 17).

3.2 Definitions

Before diving into further analysis, a range of terms within medical devices and cybersecurity must be clarified.

3.2.1 Medical Devices

Outside of legal definitions, medical devices can be understood as machines, tools, software, or otherwise, which are used in some medicinal capacity. The concept covers both what is used by healthcare professionals, as well as patients, which makes great sense in the context of medical treatment and philosophy understood broadly.[37] Medical devices are extensions of the action of restoring health, and while they cannot alone bring about healing, they are often a core part of the supply chain of treatment. In Section 3.3.1 and 3.3.2 they are defined within law, and this definition, or understanding, is what is used throughout the thesis.

Surgical Robots as Cyberphysical Systems and Medical Devices

Surgical robots[38] are cyberphysical systems (CPS), which means they seamlessly integrate computation and physical components into their operation.[39] A generic description would be that the lowest level starts with sensors and actuators, which are connected to a field or a sensor network, all of which would be managed by a control system, that itself would be

[37] Fredrik Svenaeus, *The Hermeneutics of Medicine and the Phenomenology of Health: Steps Towards a Philosophy of Medical Practice* (2nd, The International Library of Bioethics, vol 97, Springer International Publishing 2022) ⟨https://link.springer.com/10.1007/978-3-031-07281-9⟩ accessed 11 July 2023.

[38] An example of the first generation of actual robotic surgical systems, could be the experimental PUMA 200 manipulator from 1988, which would define entry orientation and location of a surgical needle. The operator would then insert the needle as defined by the robot, Bergeles and Yang (n 17) 2.

[39] NSF (n 24) 2.

bound to a control system network.[40] The human machine interface would exist at this level, which would be where the operator of a surgical robot would reside. Autonomous cars, smart grids and IoT devices are all included in these criteria, but with these features come many vulnerabilities, which are included with the connection to a network or the internet. As they have physical components, these devices can interact and affect the health of humans, and so can an adversary that successfully attack the system. This becomes even more important to consider as surgical robots are considered patient safety-critical, just like a normal surgeon during surgery would be, because of the potential risks imposed on the patient.[41]

CPS consists of many hardware and software systems combined, and each can be manipulated from the outside, even if it is loosely isolated from the internet.[42]

Essentially, it is assumed that surgical robots are CPS, which is used to connect it and this chapter to the wider field of CPS as some of the legal considerations can apply to other systems which interface with humans in the same manner.

Surgical robots are medical devices because they fulfil the legal requirements which will be introduced below, but also because they fulfil the same role as traditional medical device equipment does during surgery. The parallel to scalpels is poignant, as surgical robots possess these and other independently existing medical devices, and create new opportunities for the surgeons, and therefore also the patient. By both deploying and enabling new or existing surgeries, and therefore paths towards healing, surgical robots are by themselves, even if disregarding legal requirements,

[40] Kazukuni Kobara, "Cyber physical security for Industrial Control Systems and IoT" (2016) E99D(4) IEICE Transactions on Information and Systems 787.

[41] Homa Alemzadeh and others, "Adverse events in robotic surgery: A retrospective study of 14 years of fda data" (2016) 11(4) PLoS ONE 1, 15.

[42] Kobara (n 40) 788.

medical devices.[43]

The two terms, active surgical robotics and telerobotics, are closely related and generally explain what is seen as surgical robots. Active surgical robotics means robots with pre-programmed data and computer-generated algorithms that function without real-time operator input.[44]

While also containing these features, telerobotics additionally emphasizes a remote control of a robot by a human. Control of the robot can be completely manual, or supervisory, the latter requiring substantial intelligence and/or autonomy for the robot.[45] A telerobotic system has an operator-site and a remote-site. The operator-site usually has an acoustic display, a visual display, a tactile display, and a haptic display. Remote-site usually has acoustic, visual, haptic, and kinesthetic-tactile sensors or actuators. Remote-site is most often in the same room or very close to the operator-site. For this chapter, the focus is on telerobotics, which will be called surgical robots since they currently all require a network connection to function properly.

3.2.2 Adversarial Failures

Given the extensive developments in CPS, it could be difficult for manufacturers, doctors, hospitals, robot operators, engineers, lawyers, and policymakers to fully keep up with developments. As these solutions become popular, there is ever greater need to understand how they fail, since this is fundamental to any litigation and assignment of responsibility.

Adversarial failures are caused by an active adversary who attempts to induce failures to attain their goals, such as manipulating the surgeon's

[43]Bergeles and Yang (n 17).

[44]NG Hockstein and others, "A history of robots: From science fiction to surgical robotics" (2007) 1(2) Journal of Robotic Surgery 113, 114.

[45]Günter Niemeyer, Carsten Preusche, and Gerd Hirzinger, "Telerobotics" in *Springer Handbook of Robotics* (Section: 31. 2008) 742.

commands, inferring from the surgical procedure to compromise patient privacy, or the infringement of intellectual property, such as the robot's algorithm, or trade-sensitive data like the surgeon's inputs. There are other taxonomies for security[46] and safety,[47] but a separate taxonomy is needed due to the specific issues that surgical robots pose. There are close similarities between IoT and surgical robots, but not enough to warrant using the same taxonomies. Specialised types of CPS require their own considerations.

Taxonomy for Surgical Robotic Adversarial Failures

Adversarial failures of anything within cybersecurity can be described in various manners; for surgical robots, a simple taxonomy should encompass what is relevant and proven in practice and include a speculative category that may become more prevalent in the future.
The proposed categories of adversarial failures for surgical robots are therefore as follows:

1. *Manipulation Attacks.*[48] The adversary covertly modifies the instructions to get a different desired response. This is understood in the broadest sense, since it can be initiated in any part of the CPS

[46]See some of them in the following 5 examples: Syed Rizvi and others, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT" [2018] Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018 163 (ISBN: 9781538643877 Publisher: IEEE), Davide Quarta and others, "An Experimental Security Analysis of an Industrial Robot Controller" [2017] Proceedings - IEEE Symposium on Security and Privacy 268 (ISBN: 9781509055326), Dorottya Papp, Zhendong Ma, and Levente Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy" [2015] 2015 13th Annual Conference on Privacy, Security and Trust, PST 2015 145 (ISBN: 9781467378284), Taimur Aslam, Ivan Krsul, and Eugene H Spafford, "Use of A Taxonomy of Security Faults" [1996] Proceedings of the 19th National Information Systems Security Conference 551 and Carl E Landwehr and others, "A taxonomy of Computer Program Security Flaws" (1994) 26(3) ACM Computing Surveys (CSUR) 211.

[47]Milos Vasic and Aude Billard, "Safety Issues in Human-Robot Interactions" (2013).

[48]The word attack is used here, regardless of whether it is a failure, for historical reasons.

that surgical robots consist of.[49] The attacks can be injections of unintended user inputs, or motor torque commands, which require access to the master console or control software. The effect of this failure are unintended jumps, movements or for the robot to completely stop.

2. *Subverting robotic control.* The adversary hijacks or otherwise makes changes in the robot's control. This is different from manipulation, since this can be done on the network the robot receives signals from, and focuses on the control, not manipulating existing actions. A practical test worth mentioning,[50] where packets were delayed or changed between the operator and robot, and using this technique, they were also able to hijack the surgical robot. This was done by fooling the robot to believe that input packet loss was occurring, but not long enough to interrupt the operation, and the surgical robot would then only be able to be controlled by the packets sent by the adversary.

3. *Reprogramming the robot.* The type of access that is needed to manipulate the robot may also allow access to change the software as well.[51] The failure consists of changes in software on any level, and while there are currently no practical examples for surgical robots, the severity of such failures on the patient or operation in general is large enough to raise concern. The possible enabling of other failures or other newly programmed actions are great too, and this only

[49]This was tested in practice on the RAVEN II open platform, which is similar to current surgical robots, see Alemzadeh and others (n 27).

[50]Tamara Bonaci and others, "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots" [2015] 1 (_eprint: 1504.04339) ⟨http://arxiv.org/abs/1504.04339⟩.

[51]This is a typical and well-known concept in security, see e.g., Gamaleldin F Elsayed, Jascha Sohl-Dickstein, and Ian Goodfellow, "Adversarial reprogramming of neural networks" [2019] 7th International Conference on Learning Representations, ICLR 2019 1 (_eprint: 1806.11146).

shows how important maintenance and routine validation of equipment is.

4. *Misappropriation of trade secrets.* This is seen as the attackers recreating the underlying technique of surgery by collecting surgical control instructions over time. This failure can be initiated over the network or inside the surgical robot, resulting in a loss of confidentiality. While it cannot harm the patient, it is misappropriation of the techniques used by surgeons currently and could in the future constitute the basis for data sets that AI or machine learning algorithms can use to replace the operator entirely. Collecting this without the consent of the surgeon is both unethical, likely violates rules on trade secrets and constitutes an issue that will generally need to be addressed further on.[52]

5. *Poisoning the feedback loop.* The adversary covertly modifies the camera and/or other sensory outputs sent to the surgeon. Sensory inputs are currently vital for showing where the procedure inside the patient is at, as well as what the surgeon is currently doing. If any of these are changed, the risk of injury of the patient increases. The difficulty of resetting or returning the robot to its initial position is further hampered by any feedback being off or wrong, which makes this a dangerous failure.

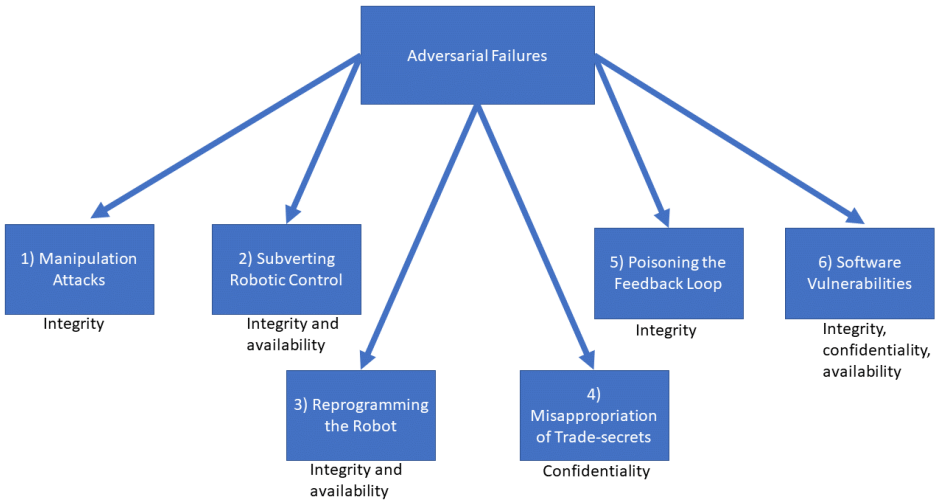
6. *Software vulnerabilities.* Any vulnerability that an adversary can make use of to commit further attacks on, is considered a failure as such. It is also the broadest since it covers any part of the surgical

[52] See early indicative work like Sharon K Sandeen, "Out of thin air: trade secrets, cybersecurity and the wrongful acquisition tort" in Tanya Aplin (ed), *Research Handbook on Intellectual Property and Digital Technologies* (Edward Elgar Publishing January 2020) ⟨https://china.elgaronline.com/view/edcoll/9781785368332/9781785368332.00025.xml⟩ accessed 13 January 2024.

robot and its accessories. Unlikely the failures above, this is passive and not necessarily caused by the adversary, but instead enables them to cause failures because of it.

The taxonomy is illustrated in the following figure.

Figure 3.1: Illustration of adversarial failures for surgical robots, which includes what is compromised, here integrity, confidentiality, and availability.



Safety Failure Issues

Non-adversarial failures are not discussed in detail in this chapter, but they are listed for completeness. This enables later safety centred analysis of surgical robots and medical devices to make use of the ideas presented.

Non-adversarial failures are caused by the correct operation of the surgical robots as per the specification, but where an unsafe outcome is caused nonetheless. These can be seen as:

1. The robot works in unintended ways because of failures in motor calibration or sensory defects.

2. The robot causes a denial of service on itself whilst legitimately trying to accomplish the assigned task.

3. The robot has an incremental bias which creeps in due to shifts in belt tensions, gear wear-and-tear and other electro-mechanical causes.

4. The robot fails to handle shifts in lighting, shadows, tilt of surface level, noise, mist or other environmental noise in the visual or acoustic plane.

5. The robot fails to perform due to inability to function in poor network conditions or being operated in network conditions (jitter, throughput, and bandwidth) that are quite different from what it was tested on.

Adversarial failures can manifest via non-adversarial pathways. An attacker may manipulate neighbouring devices that are not connected to the robot via a computer network but nonetheless provides interaction pathways. For instance, an attacker may introduce subtle changes in lighting via a compromised IoT lightbulb inducing a failure in the surgical robot's image recognition component, which may lead to patient injury.

This is an example of a situation where a safety failure in the robot is induced via a compromised device in the vicinity of the said robot. In security literature, these are referred to as stepping-stone attacks, where the attack is carried out through indirect influence rather than direct engagement between the surgical robot and the attacker.[53] This approach affords relative anonymity to the attacker and makes attribution difficult, as the attacker is separated several steps away from the intended target due to the indirect nature of engagement.

[53] See e.g., David M Nicol and Vikas Mallapura, "Modeling and Analysis of Stepping Stone Attacks" [2014] Proceedings of the 2014 Winter Simulation Conference 3036 (ISBN: 9781119130536).

Adversaries

The identity of the adversary, the party that seeks to cause adversarial failures, have different priorities and foci, so it is natural to assume certain things about them, as adversaries are traditionally modelled in security.

The adversarial model used here includes cybercriminals, disgruntled employees, terrorists/activists/organized criminal groups, and nation states,[54] as well as competing surgical robot manufacturers. The widest range of actors possible is chosen, since the selection of them and which failure they want to induce can change the outcome of the analysis in the following sections.

It is illustrated in the following figure.

Figure 3.2: Illustration of which adversarial failures the adversaries induce in the context of adversarial attacks on surgical robots.

Adversaries	Cybercriminals	Disgruntled Employees	Terrorists/activists	Nation States	Competitors	Organized Criminal Groups
Adversarial Failures						
Manipulation Attacks	X		X	X		X
Subverting Robotic Control	X		X	X		X
Reprogramming the Robot	X		X	X		X
Theft of Trade-secrets		X		X	X	X
Poisoning the Feedback Loop	X		X	X		X
Software Vulnerabilities				X	X	

It is assumed that stronger players can induce many failures, while competitors and disgruntled employees would only induce a few. Any attacks that can cause injury from those two are left out, since none of them would have the intention to cause them in the first place. Cybercriminals and

[54] Alvaro A Cardenas and others, "Challenges for Securing Cyber physical Systems" (2009) 2009(3) Computer Audit Update 3, 1 - 2.

organized criminal groups overlap and can generally both create all failures except for software vulnerabilities, but it can be assumed that misappropriation of trade secrets would be done only by the organized party. Terrorists/activists would want to create as much of as much disruption as possible, which is why they would go for failures that cause this. And nation states are capable of everything, with the highest number of resources at their disposal.

3.3 European Sources

The following section introduces and analyses relevant EU legal sources. It does so with a focus on manufacturers and authorities, and generally gives both an overview of the MDR, but also some in-depth commentary which is necessary for the sections that follow it.

3.3.1 Medical Device Directive

MDs are as of the time of writing no longer governed by the MDD. From the end of May 2021, the MDD became obsolete, but it continues to be a source of regulatory inspiration because of its similarities to the MDR and its historical significance, so it is addressed here.

The term "software" is only mentioned twice in the Directive. One of these places is in Art 1(2), where software is included if it is *"necessary for proper application intended by the manufacturer to be used for human beings."*[55] Any software then has to be an *"instrument, apparatus, appliance, material or other article,"* and be intended for certain purposes. These are:

[55] In a rephrased fashion, the same purposes must be fulfilled in the directive as from Art. 2(1) in the MDR.

1. Diagnosis, prevention, monitoring, treatment, or alleviation of disease,

2. Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,

3. Investigations, replacement, or modification of the anatomy or of a physiological process,

4. Control of conceptions.

These must not achieve their main goals in or on the human body by pharmacological/immunological/metabolic means,[56] and this is because these devices may be regulated by the in vitro MD regulation (or 'IVDR') instead.[57] Software must therefore be treated and evaluated according to the same rules as every other MD, if covered by the jurisdiction of MDD. Software can also be considered an accessory to a MD, and in such cases must fulfil the same requirements as the MD, see Article 1(2)(b).

Unlike the Regulation, the MDD was a directive, which entailed a different implementation of the directive in each EU Member State.

Some of the criteria are similar to what can be seen in the new Regulation. However, given the direct effect of the Regulation's provisions compared to the transposition of the Directive into national legal systems, there may be divergence between past practice under the MDD and new practice under the MDR within a particular Member State's national jurisdiction.

There is no explicit article on scope and subject in the MDD, but Article 2 shows that a primary purpose of the Directive is the placement onto the market of MDs, but only if they do not compromise the health of the

[56] See Art. 1(2)(a). They can assist in achieving these main goals, but cannot be the principal way to achieve it.

[57] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU OJ L117/176.

patients, users, or other persons when used for their intended purposes. The rest of the structure resembles that of the MDR in a shorter and more concise form.[58] Since the MDR is more comprehensive, a more detailed overview of it is given below.

3.3.2 The Medical Device Regulation

The MDR is designed to achieve a balance between a high level protection of health for patients and users, as well as ambitious standards for quality and safety of medical devices.[59] This fits the scope of the regulation, stated in Article 1(1), which is a focus on laying down rules for placing medical devices on the market.[60]

As an EU regulation, it is applicable directly through its literal wording, unlike directives which are required to be implemented into national law. The scope of the Regulation seen in Article 1(1), is to define rules for MDs in the three senses of *placing on the market, making available on the market, put devices into service for human use and accessories.*[61]

This means that the subjects and the core focus of the Regulation are the devices, and therefore also their manufacturers and anyone else that sells or distributes them. They must as subject of the Regulation play a substantial part in complying with the rules, self-evidently identifying, and loyally fulfilling their duties, which follow from Article 1(1) and Article 10(1). The jurisdiction of the MDR vis-à-vis manufacturers is potentially world-wide. According to Article 1(1), any manufacturer, regardless of where they are located, that wants to enter the European Single Market must con-

[58] The MDD only has 23 articles compared to the 123 of the MDR.

[59] See the MDR, preamble 2.

[60] Contrary to a directive, a regulation is a binding legal instrument that is directly enforceable by the states and the EU, see Art 288 in the Consolidated Version of the Treaty on the Functioning of the European Union.

[61] This is deeply contrary to Art. 2 of the MDD. The MDR does not mention safety or health in its scope article.

form with the MDR. The term software is mentioned in the Regulation,[62] but is not treated separately nor are there any specific articles concerning it. The general rules for MD therefore apply to software and hardware. Article 1(1), on subject matter and scope in the Regulation, does not literally exclude software as being considered a "medical device for human use", and it is not excluded in Article 1(6) either. In the Regulation's definitions in Article 2(1), software is mentioned as a MD if it used for either or several of these purposes:[63]

1. Diagnosis, prevention, monitoring, prediction, prognosis, treatment, or alleviation of disease,

2. diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,

3. investigation, replacement, or modification of the anatomy or of a physiological or pathological process or state,

4. providing information by means of in vitro examination of specimens derived from the human body, including organ, blood, and tissue donations.

As with the MDD, software can also be an accessory to a MD.[64] The MDR makes a sharp distinction between software intended for use with or as a MD and software for general purposes (preamble 19). If not intended to be used with or as a MD, generic software, which is defined as software for general purposes, can never be an accessory or a MD. If it is specifically intended by the manufacturer to be used as such (but is not generic), it may be considered a MD or an accessory if it fulfils the other requirements.[65]

[62] See preamble 19, Arts. 2(1)(4)(25)(26) and in the annexes.

[63] These resemble those seen in the MDD but are slightly different in wording.

[64] Article 2(1).

[65] Software which is a MD or is an accessory must also have and display a CE marking, see Article 20.

Like with the MDD, before Article 2(1) applies, the software must be intended by the manufacturer to be used for the listed means. This makes the evaluation of whether there exists such an intention a gatekeeper as to whether the MDR even applies in the first place.

In the view of the safety concerns of the public and manufacturers, the character of the MD is to be assessed before it is released onto the market. This is done through classes that designate increasing levels of risk. MD are divided into class I, IIa, IIb and III, as per Article 51(1). The determinations of these classes are defined in Annex VIII in the MDR. The difference in class can be seen as reflecting the danger a MD poses to those it is used on, be it patients or users, which results in special rules given to the higher classes. For class III, this would include Arts. 27, 32, 52, 54, 55, 61, 86 and 105.[66] Software is mentioned in Section 3.3 of Annex VIII, which dictates that if it drives or influences a device it shall have the same class.

However, even if the software is independent, it must still be classified with regard to its potential danger to the workflow that can affect the patient. Specific rules follow these two principles. Rule 11 in Annex VIII assumes at first that all software that is also a MD is class I.[67] The exception to this is software which is used to take decisions on diagnosis or has therapeutic purposes. These are instead considered to be class IIa. The exception to the exception would be if the software can cause serious deterioration of the health of a person, which makes it class IIb, or if it is capable of causing death or irreversible deterioration to the health of a person, in which case it is class III. If the software monitors physiological processes, it is class

[66] Some of these articles contain other rules, like Art. 32, but they are listed because they include special obligations for manufacturers of MD that are class III.

[67] Such as Google's latest attempt to launch a Disease Diagnosis Software in the EU, which is as of the time of writing Class I, see https://blog.google/technology/health/ai-dermatology-preview-io-2021/amp/, last accessed 11 December 2024.

IIa, but if it can cause immediate harm to the patient during its use, it is to be considered class IIb.

The MD regulatory framework in the EU is enforced by nationally appointed regulators in each Member State in Article 101. The Medical Device Coordination Group (MDCG), an innovation of the MDR, see Article 103, is the new organ that facilitates cooperation between the different regulators, but it is not by itself the central authority. The national authorities can make use of a wide array of enforcement tools, including forceful withdrawal and banning of a MD as seen in Article 10(14). For the purposes of this chapter, the market surveillance activities done by the regulators seen in Article 93 is central as well. This kind of surveillance can include a focus on software distribution platforms, and while it focuses on devices,[68] this does not exclude evaluations of whether software already considered MDs cannot later be excluded based on not fulfilling Article 2(1), especially with a focus on intention. A search for further information about national authorities' practices in utilising their regulatory powers under the MDD was undertaken, however, information about these practices is either not publicly available or does not exist, which makes evaluation of their past regulatory behaviour and prediction of future behaviour difficult. Whether and how the regulators evaluate the intention of the manufacturer *ex ante* is also unclear and unknown.

National regulators in the EU do not always assess the conformity of the devices initially before they enter the market. This activity is at first left to something called a notified body.[69] These are usually private companies, which are given the competence to assess MDs. Software submitted to a notified body may confirm the intention of the manufacturer, as submitting one's product to such a body is akin to admitting it is a MD directly or

[68] See Art. 93(1).

[69] See Art 35 and 36.

implicitly. However, if the software is not admitted after being assessed by the notified body, it is not a medical device, regardless of the opinion of the manufacturer.

Manufacturers

Surgical robots can be put on the market by several different parties.[70] As a general rule, the manufacturer answers only to the regulator in its place of business.[71] However, any patient in any member state can sue any manufacturer, because of the rule of special jurisdiction.[72]

The central obligations for the manufacturers are the following:

1. The system of risk management (Article 10(2)).
2. The system for quality management (Article 10(9)).
3. Sole responsibility for devices (Article 10(1)(12)(13)(14)).
4. A system for financial responsibility (Article 10(16)).
5. Annex I specific obligations.

The system of risk management. This is also defined in Annex I, section 3. The regulation defines it as a continuous iterative process through the surgical robot's entire life cycle. The system has to identify and analyse all foreseeable hazards, estimate and evaluate risks associated with or occurring during intended use and the future, eliminate or control those

[70] Such as importers and distributors, see Art 13 and 14.

[71] See Art 10(14).

[72] See Art 7 in Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters [2012] OJ L 351/1.

and evaluate this information and combine it with the data gathered from the post-market surveillance system.[73]

The term hazard does not literally include adversarial failures, but since they can cause hazards in a safety manner, like the surgical robot jumping or possible getting hijacked which risks the patient and anyone nearby, they should naturally be included. Misappropriation of trade secrets or software vulnerabilities cannot directly cause physical harm, and should therefore not be included, unless they clearly cause further adversarial failures. From this, all other adversarial failures mentioned in the framework earlier, must be eliminated or controlled.

The system of quality management. While this system includes the risk management above, it also has other elements. Firstly, identification of applicable general safety and performance requirements/exploration of options to address it. This is mandated,[74] and must be addressed separately from the rest. Secondly, the post-market surveillance system, which in security terms must identify all incidents that can occur to the surgical robot in the future. As both angles must imagine all types of safety failures, any kind of security failure, by an adversary or otherwise, must clearly be included.

Sole responsibility. The term sole responsibility refers to the manufacturer's role as both the creator and controller in Article 10(12), in the sense that any non-compliance by the device has to be relayed to the regulator, and as a partner with the regulator, since they have to cooperate and follow requests given in Article 10(14). This refers back to Article 10(1), which solely states that the devices should be designed and manufactured

[73] As seen in Art 83, which requires manufacturers to have a system in place for surveillance of the post-market situation of their device, be it academic or technical data.

[74] See Art 10(9).

to comply with the regulation. Generic software, other than it being updated, is not included, but accessories are. This is a straightforward way to show liability in national law in the case of doubt, as it constitutes a legal rule which will be breached if the surgical robot suffers an adversarial failure that could have been prevented or mitigated. It can also be further expanded to include notions of safety failures and security breaches.

A system for financial responsibility. This is defined in Article 10(16), where compensation schemes specific to each country are mentioned, which usually involves initial insurance coverage, but also product liability lawsuits and national law. The risk class, type and size of the manufacturer plays a role in which measures, like insurance, that they have to undertake, but the article takes national protective measures into account. This shows that the regulation leaves all legal remedies and considerations concerning litigation up to the member states and insurance solutions, which detracts from its value as a regulation, because it reduces the effect of the proposed harmonisation.

Annex I. This annex further defines requirements for the medical devices, and according to the guidance and if read literally, section 17 on electronic programmable systems, should be the focus when it comes to surgical robots. Section 17.1 requires that the devices be designed for repeatability, reliability, and performance. If a single "fault" is found, it has to be eliminated or reduced as much as possible. Whether fault only refers to non-adversarial failures or the opposite is unclear, but considering the guidance's emphasis on this part, an interpretation that sees it as adversarial failures seems appropriate. This is supported by safety faults being the focus elsewhere.[75] Since these requirements are not part of the risk man-

[75] See e.g., Chapter III, Annex I.

agement system, this further emphasizes that preventing any adversarial failure besides misappropriation of trade secrets, and repetition of these requirements in different ways cements its importance in the production, sale, and usage of surgical robots. Section 17.2 of Annex I require the software used in devices to be developed/manufactured with the "state of the art". State of the art is used sparingly in the regulation but has not been included in any of the central articles. The term in section 17.2 equates to regular updates and maintenance of the software, and it has to consider the life cycle of the device and *information security, verification and validation* of the robot. The three last categories would imply that it should catch all adversarial failures, with security preventing manipulation attacks and subversion of robotic control and perhaps misappropriation of trade secrets, and verification catching reprogramming of the robot and poisoning of the feedback loop, and validation reinforcing whether the security is adequate or not. State of the art would then prevent software vulnerabilities by regularly identifying and erasing them. However, state of the art only requires what term encompasses, which also means that anything that the industry does not know or what is not expected of it, it does not require the manufacturer to do. This includes which adversaries that should be defended against, with nation states being impossible to include because of their immense power.

Section 17.4 requires that the manufacturers decide on minimum requirements for hardware, network characteristics and security measures, which allows the software to run "as intended". This allows the manufacturer to technically set standards that could be problematic in the long run, since it might not prevent more complicated and dangerous adversarial failures.

Authorities

The regulator is defined as the competent authority, which Member states designate themselves.[76] As with manufacturers, a range of rights of the regulators which are relevant when considering surgical robots and which will affect the responsibility and liability of the manufacturers are discussed.

1. Right to request documentation and punish the manufacturer if they do not cooperate (Article 10(14)).

2. Market surveillance activities (Article 93).

3. Evaluation of devices suspected of presenting an unacceptable risk or other non-compliance (Article 94).

4. Procedure for dealing with devices presenting an unacceptable risk to health and safety (Article 95).

5. Other non-compliance (Article 97).

Right to request and punish. This part of the article contains the special right for the patient in its paragraph 3, but focus should be on 1 and 2. In paragraph 1, the manufacturer must provide documentation to demonstrate conformity of the device, or samples free of charge or access to the device. Further, they have to cooperate on any corrective action to eliminate or reduce risk for devices they put on the market.
If this is in some way not possible, the regulator has the right in paragraph 2 to take all appropriate measures to prohibit, restrict, withdraw, and recall the device.[77] The right is not built up as an immediate use of force, but

[76] See Art 101.
[77] See Art 10(14), second paragraph.

rather the opposite. It is instead based on trust in the manufacturer fulfilling the requests from the regulator dutifully. It is not specified whether the regulator has the necessary knowledge or personnel to request actions or documentation that relates to security, but because of the existence of the guidance this may be the intention.

While this is not a liability for the manufacturer, it constitutes a risk of their product being banned or forcefully withdrawn or changed - all of which are increased costs and gives extensive powers to the authorities.

Market surveillance activities. This activity resembles what most are familiar with from national food regulation authorities.[78] Review of documentation, physical or laboratory checks are possible, as is requesting documentation from other parties than the manufacturers and unannounced inspections.[79] How this can be applied to security cannot be literally read, but considering the wide power the regulator has, it is theoretically able to thoroughly review and inspect risks that might lead to adversarial failures.[80]

Evaluation of non-compliance. If the regulator takes notice of there being an unacceptable risk to the health, safety of patients or others, or if the device seems to not comply in general, they are then allowed to carry out a more thorough investigation that includes the complete check of compliance of the regulation.[81] It is unknown whether this includes penetration testing or other validation measures of the devices.

[78] See e.g., Chapter II in Regulation (EC) No 853/2004 of the European Parliament and of the Council of 29 April 2004 laying down specific hygiene rules for on the hygiene of foodstuffs [2004] OJ L139.

[79] See Art 93.

[80] This is both promising, and at same time most likely a huge weakness of the MDR.

[81] See Art 94.

Procedure for devices that risk health and safety. If the regulators are confirmed in their suspicions, they first ask the manufacturer to take all appropriate and duly justified corrective actions to restore compliance, and until then, themselves proportionally restrict the availability of the device.[82] This latter point means recalling the device in practice. And if this is not done, this reverts back to Article 10(14), where the regulators can forcefully remove the robot from the market.

Procedure for non-compliance. If the evaluation showed other non-compliance, the regulator could react in a similar fashion to Article 95. The requirement for unacceptable risk to health and so on, is not present here, but the powers are the same. This is interesting because it can potentially include adversarial failures that do not have a risk to the health and safety of anyone, for example misappropriation of trade secrets and software vulnerabilities. It remains to be seen how this can be used in regard to surgical robots.

Accessories

Like other robots and CPS, surgical robots make use of software and physical additions that on a practical level will be accessories. But there are certain requirements for them to be considered accessories in regime of the MDR. The reason why identification of these is important, both to a manufacturer and to a potential injured patient, is because many of these could be points of entry for adversarial attacks, or be the actuators that injure the individual or the operator.

Accessories of surgical robots are governed by the same rules as the robots they are used with,[83] even if they do not attain the status of MDs. It must

[82] See Art 95.
[83] See Art 1(1).

be defined what accessories are in this context as stated in Article 2(2), because a surgical robot as a system has more accessories than most MDs, which puts it in a unique position in terms of liability for the manufacturer. Any tools that are themselves already MDs are excluded, such as the scalpels and other tools used by surgical robots, which will be covered by Art 2(1) just like the robot itself, and even if they practically are accessories.[84]

Any traditional accessory that is not a medical device, such as sensors for surgical robots, are included in Article 2(2), first definition. But the second definition expands and includes anything that exists "to specifically and directly assist in the medical functionality of the medical device(s)." To be considered an accessory, it therefore has to also specifically and directly assist with the medical functionality of the surgical robot. For telerobotic surgery this is both the encrypted connection, the local network that enables it and the operator screen and equipment that controls it elsewhere. This is therefore an expansion of what an accessories means in a medical device context.

This does not mean that the accessories, if not directly a part of the surgical robot, make the manufacturer specifically responsible. The operator or end user must maintain and keep them updated,[85] and a separate evaluation on whether they would be considered medical devices is taken by the member state.[86] The relevant national regulatory authority is that of the accessory manufacturer's place of business, as is the case later in this chapter. But if the accessories, such as specific equipment for the physical part of the surgery, are a direct part of the robot, and is not included in

[84]Huu Minh Le, Thanh Nho Do, and Soo Jay Phee, "A survey on actuators-driven surgical robots" (2016) 247 Sensors and Actuators, A: Physical 323 (Publisher: Elsevier B.V.) ⟨http://dx.doi.org/10.1016/j.sna.2016.06.010⟩.

[85]Depending on the contract between them.

[86]See preamble 8.

the exception in preamble 19 of the MDR, the manufacturer is responsible for any safety or security issues they present. Whether this covers both the original manufacturer of the accessory, such as developers of modified software or original manufacturers of actuators, is not clear from the MDR alone.

This expansion of the concept of accessories regarding surgical robots increases the amount of possible targets for lawsuits from the patient, since software or actuators that are accessories but which may have initially suffered an adversarial failure to allow access into the surgical robot itself, will bear their own liability alongside the manufacturer of the surgical robot.[87]

At its core, accessories will have their own known adversarial and non-adversarial failures, which the manufacturer may be responsible for either through Article 2(2)(1), non-medical devices which enable the medical device, or Article 2(2)(2), non-medical devices who specifically or directly assist a medical device. From this, 5 categories of specific accessories for surgical robots can be created, which combine the real complexity which is surgical robots as CPS with the flexibility of the MDR, to allow future authors to explore the very thin veil between the manufacturer of the entire CPS being liable, versus when the manufacturer of the accessory is.

These categories are illustrated in the following figure.

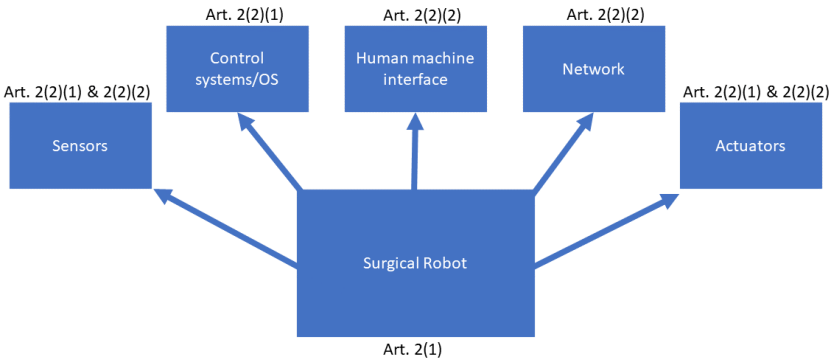
3.3.3 Guidance

Like national law, EU law has additional documentation and guidance that can be used by different parties affected by it. One of these the is "Guidance on Cybersecurity for medical devices",[88] which is issued by the Med-

[87]The scope of this chapter does not allow these observations to be fully discussed, for more details see section 3.7 below.

[88]For a separate commentary on this, see Elisabetta Biasin and Erik Kamenjasevic, "Cybersecurity of Medical Devices: Regulatory Challenges in the EU" in *The Future of*

Figure 3.3: Figure which illustrates accessories of a surgical robot.



ical Device Coordination Group (MDCG).[89] In general, guidance can be seen as legally binding,[90] a tool to guide interpretation or at least act as guidelines for the parties.

The MDCG, while having created this, does not issue legally binding guidance, as there is nothing stating this in the MDR, but Article 103(8) does allow them to create recommendations or opinions in emergencies. For this reason, it seems legitimate to view the guidance on security as non-binding soft law.

While the MDR does not explicitly consider the safety to security problems, this guidance does on page 10. It equates security risks having a safety impact, which here for us would refer to damage to a patient caused by an adversarial failure. It argues that because of this, Annex I[91] has to both be interpreted in a safety as well as a security manner. This dispels any doubt whether the MDR can be used to argue for lawsuits on the basis of adversarial failures.

Medical Device Regulation: Innovation and Protection (2020).

[89] Established by Art 103 in this regulation.

[90] This is prevalent in e.g., Danish law, if the guidance is purely made for a specific public authority, but can be problematic to always impose in EU-law, as it relies on national authorities and interpretations entirely.

[91] Defines further requirements for medical devices.

Meddev 2.1/6 and MDCG 2019-11

Two other central pieces of guidance must be mentioned before moving forward. These diverge, as they pertain more to question of when software is a medical device or not.

Issued with the MDD, is the 'Guidelines on the Qualification and Classification of Stand Alone Software used in Healthcare within the Regulatory Framework of Medical Devices,' known as MEDDEV 2.1/6 for short. Only some points which are important to our discussion are covered, as the guidance also contains several outdated passages.

Issued as guidance before the MDR came into force, 'Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR', called MDCG 2019-11, is the updated guidance on software as MD.

Since MEDDEV 2.1/6 was built around the MDD, it did not contain many specific articles from which inspiration can be drawn. It does add that generic software should not be considered a MD if it is part of several software modules in one unit.[92] Every evaluation of such software must be individual (for each type of software), and so the fact that one module is a MD does not also make the entire system one as such. A central limitation of this guidance is that it only applies to standalone software[93] and not software incorporated in MD such as those seen in surgical robots. But this does not limit its role for inspiration for interpreting the MDR in the future, together with the new guidance. The MEDDEV 2.1/6 assures that the intent of the manufacturer plays a central role, regardless of what the software is called.[94] This can be interpreted as the situation where the software may be called something in regard to healthcare, but the intent

[92] See p. 20 – 21 of MEDDEV 2.1/6.
[93] This term is no longer used, see MDCG 2019-11, footnote 2.
[94] P. 8 of MEDDEV 2.1/6.

from the manufacturer was purely for the software to act as something informal. The choice of operating system that the software runs on does not affect the evaluation of the software either, or the risk of malfunction of software run in a medical environment does not make into a MD *per se*.[95]

The guidance includes a "decision diagram to assist qualification of software as medical device".[96] The MDCG 2019-11 has a slightly updated diagram[97] that can be used for inspiration. The diagram states that if the software does not fulfil the criteria, it is not covered by the MD directives, which is interpreted as meaning that the software is not considered to be a medical device. This has been clarified in the new guidance.

Here the aspects of the diagram relevant for this chapter are identified:

1. The first point relates to whether the software can be defined as software in the guidance. Related to the MDR, there is no stringent definition of this. This is in itself tautological.

2. The second point relates to whether the software is standalone or not. If it is not, it can either be part of a MD or not covered by the MDD.

3. The third part defines that if the software merely acts on data from storage, archives, communication, or simple search, it is not a MD.

4. The fourth part postulates that if the actions of the software are not for the benefit of individual patients, it is not a MD. Note that neither MDD nor MDR has the benefit of patients as among their explicit main purposes.[98]

[95] Ibid, p. 9.
[96] Ibid, p. 10.
[97] P. 9 of the MDCG 2019-11.
[98] But MDD does it have it in Art. 2.

5. The fifth part says that if the software does not fit a purpose contained in Article 1(2)(a) of the MDD, it is not a MD, and it is if it does. But even if it is not a MD, the software can still be considered an accessory, which would lead to the same requirements as that of a MD.

6. The sixth part says that to be an accessory, the software must fulfil Article 1(2)(b), which means that it must be intended specifically to be used with a MD by the manufacturer. Otherwise, it is not a MD or an accessory at all.

As the keen reader would have noticed, while the whole diagram is interesting for inspirational and historical reasons, the fourth point stands out. The MDR does not include as a criterion whether a MD benefits individuals, it is not even mentioned literally in the text. It instead considers whether the devices are for human use.

MDCG 2019-11 repeats several of these requirements in its diagram and text, but it is notably different. MDCG 2019-11 does not view software in modules, and instead focuses on whether it fulfils the requirements to be a MD by itself, if it drives or influences a MD, regardless of where it is, and if used explicitly for a MD related purpose by staff or lay persons.[99] This last point is unique and has no basis in the MDR. The guidance further simplifies the decision diagram from MEDDEV 2.1/6,[100] and differs with this and the lack of reference to the MDR's Article 2(1) – instead, opting to refer to its own definition of Medical Device Software.[101] The definition of software here is "a set of instructions that processes input data and creates output data", which is not how the term 'software' is viewed in EU law or

[99] P. 7 of MDCG 2019-11. The example in the document is insulin injection, whether via electrical pump or manually via syringe.

[100] Ibid p. 9.

[101] Ibid p. 5 and 7.

general definitions of software otherwise. Accessories to MDs for example may not input and data and create outputs, yet they are covered by the MDR regardless.

As can be seen, these two guidance documents veer off what the MDR is capable of prescribing to manufacturers of medical devices; this has implications for future guidance specifically for cybersecurity. It also showcases how accessories can be understood in the ecosystem of medical devices, though this is still partially undecided.

3.3.4 Case Law

One central case must be analysed before we can move on to discuss a possible solution to prevent circumvention in the MDR.

A fair number of cases have been decided on by the CJEU (Court of Justice in the European Union) in regard to MDs.[102] However, most of these do not concern software, but there is one that has an influence on both MDD and MDR. The case, C-329/16 SNITEM,[103] was a preliminary ruling by the CJEU on the correct interpretation of the MDD.[104] The recent nature of the ruling makes the decision of great relevance for the MDR and its interpretation. The case concerned one question with two core points.

First, whether standalone software which gave "medico-social establishment support for determining a drug prescription" could show that it was a MD.[105]

Second, whether a MD has to act in or on the human body to be considered

[102]For example, the three verdicts on transparency in regard to data necessary to enter the market for MDs, see Alan G Fraser and others, "The need for transparency of clinical evidence for medical devices in Europe" (2018) 392(10146) The Lancet 521.

[103]Case C-329/16 SNITEM [2017].

[104]An expanded analysis of this verdict can be found in Timo Minssen, Marc Mimler, and Vivian Mak, "When Does Stand-Alone Software Quality as a Medical Device in the European Union? - The CJEU's Decision in SNITEM and What it Implies for the Next Generation of Medical Devices" (2020) 28(3) Medical Law Review 615.

[105]C-329/16, para 20.

a MD.[106]

The CJEU answered both questions in full. According to the CJEU, the first[107] rests on what the manufacturer intended for the software to be used as,[108] and therefore whether it fulfils one or several purposes in MDD Article 1(2).

If the manufacturer intended for it to be used in this manner, it is a MD. Like now, generic software that is used in a medical setting is also clearly not a MD. Since the software supports the doctor with decision making in a manner that could affect the patient, it must be considered a MD.

The second question[109] was answered with the same legal sources as above. The Court emphasised that there is no difference whether the software has contact with a human or not, but rather what the intention of the software is; the intention of the manufacturer for it to become a MD.

The case may seem obvious with the event of the MDR, but because the MDD was a directive, it relied on national implementation and interpretation, and while this case came through relatively late, it crystallised the importance of the manufacturer's intention in the partially fragmented state that the MDD was in.[110]

With this, one can move on to the framework of intention, central to whether software is a medical device or not, and perhaps a vector by which more unsafe and insecure *de facto* medical devices can be included and regulated in practice with.

[106] Ibid, para 20.
[107] Ibid, para 21 – 26.
[108] And the consideration of whether the software is generic, referenced from preamble 6 in directive 2007/4, which amends the MDD. Equivalent is Preamble 19 of the MDR.
[109] C-329/16, para 27 – 32.
[110] Daniel B Kramer and others, "Ensuring medical device effectiveness and safety: a cross–national comparison of approaches to regulation." (2014) 69(1) Food and Drug Law Journal 1, 3.

3.4 The Intention of the Manufacturer

The manufacturer's intention, whether stated or otherwise, is central as to whether the MDR applies in the first place, which is seen in the definition of MDs in Article 2(1) and requires the manufacturer to have intended for their product to fulfil one of these enumerated purposes. This was emphasised in C-329/16. In the MDR this is further defined in Article 2(12), which states that the labelling, instructions for use, promotional material or statements made by the manufacturer in clinical evaluation is considered intended use.[111]

But how one deduces intention, besides from when it is written literally, is not clear from the MDR, nor its preparatory materials, nor past practice or the guidance. Article 2(12) does not go into detail about actual use or how the manufacturers designed the software.[112]

Therefore, a framework which can aid with this determination and increase clarity and certainty for software manufacturers and ensure consistency for regulators is proposed.

Unlike other medical equipment, the use and the design of software can be deceptive.[113] This refers to the hidden layers and the ethereal nature of software. Physical appliances (unless they also include software) have no hidden features like data collection or risks of cybersecurity breaches, but software does, so this framework is made to aid in identifying these as well.

For the MDR to be effective, it must cover all MD possible, and this framework may help all stakeholders achieve that. Of course, this framework

[111] Refers to tests conducted by notified bodies, not the national authorities initially, see Art 61 in the MDR.

[112] Even MDCG 2019-11 implies such a consideration must exist on p. 7.

[113] See, e.g., Antony Tang and others, "What makes software design effective?" (2010) 31(6) Design Studies 614 (Publisher: Elsevier Ltd) ⟨http://dx.doi.org/10.1016/j.destud.2010.09.004⟩.

lists what can be considered apparent indicative sources to determine the manufacturer's intention in regard to software as MD and can therefore not be considered an exhaustive list.

The other reason including more considerations for intention is needed, is because manufacturers stating that their software is not supposed to be a MD or not mentioning it at all, serves as the easiest way of preventing the MDR from applying. Going by the definition in Article 2(12), if manufacturers state that their software is not used for a purpose from Article 2(1), the software will not be considered a MD. But the software may very well be used by laypersons or medical professionals[114] for treatment, or it may be an app from the Google Play store that would fulfil Article 2(1) had the manufacturer labelled it as a MD. If it is purely limited to intended use, to what is available in public knowledge as Article 2(12) indicates, the manufacturer is allowed, especially of software, to circumvent the MDR, which is both a violation of the Regulation as well as a potential danger for patients, despite MDR not explicitly focusing on the latter. On top of this, if these also have poor security, the users risk further damage.

3.4.1 The Framework of Intention for Manufacturers of Medical Devices

Firstly, one must assume that the MDR did not intend for the manufacturer to be able to circumvent the entire Regulation by merely stating that their software is not a MD. Whether the MDR applies or not should instead be decided by the purposes[115] laid out in Article 2(1). If the Regulation allowed easy circumvention, it would not be able to fulfil its goals in Article

[114] MDCG 2019-11 does predict and see these types of software as being intended to be a MD, but does not specify how, when, and where, se p. 7.

[115] And not just merely whether the manufacturers intend anything or pretend not to.

1(1) and be rendered positively legally redundant.[116]

Secondly, one must expand the term intention to the *direct intention* seen in publicly available documentation and marketing materials issued by the manufacturer that concern the software. This is the concept see in Article 2(12) partially combined with even more publicly available sources. But it is here further argued that 'intention' must also include the manufacturer's *indirect intention*, which is seen in what the software is capable of, what data it retrieves or measures, and what kind of analysis or lack thereof the software is able to do. The indirect intention can therefore be considered as to what the software is capable of and what it does in practice.[117]

Indirect intention must be viewed as the actual capabilities of the software[118] regardless of what is stated in publicly available sources. To include all possible angles for this evaluation, distinctions between how the data used for usage is gathered and what the software does with the data are necessary. A third category is included, to catch software in grey areas - software that acts and functions as a medical device already.[119] However, this is not equivalent to a blanket statement which could include for example all smartphone apps just because some existing MDs which are software can run on this specific hardware. Instead, this refers to software that is capable of the same as existing MDs or which users can use directly as substitutes for existing MDs.[120]

---

[116]MDR is part of the overarching product rules in the EU, but this does not hinder special rules or considerations for highly specialised products as such.

[117]This follows the idea behind an accessory - software specifically made to support/enable other MD to function are accessories and therefore covered by the same MDR rules. Accessories are defined by their abilities, not just what they are said to be able to do, and using this terminology vis-a-vis MD as such is worth considering.

[118]US rules have a similar approach, where actual use is not perceived or included in the evaluation of MD, see Vincent J . Roth, "How much FDA Medical Device Regulation is required?" (2014) 15(3) North Carolina Journal of Law & Technology.

[119]This can be seen as the farthest extent of the idea of actual use, and it implies that there exists a similar category for accessories that are not yet considered so.

[120]Examples could be open source or freely made available software, that can be used with non-software MDs or to substitute MDs which are software, see Elisabetta Biasin and Erik Kamenjašević, "Open Source Hardware and Healthcare Collaborative Platforms:

It is considered that in the case of conflict between the two types of intention, if either indicates the intention of the manufacturer for the software to be a MD, the affirming intention will prevail. It may still after that not be a MD, because it does not fulfil any of the purposes in Article 2(1) even if the manufacturer intended for it to be so.
Firstly, the sources for discerning direct intention:

1. Information from marketing materials. If the manufacturer states that the software is a medical device, or claims it fulfils one of the purposes in Article 2(1), direct intention can be established.

2. Information from internal documentation. If the manufacturer states that the software is supposed to fulfil one of the purposes in Article 2(1) in its internal documentation to which the EU Member State national regulators or other public authorities have access due to Article 10 or other legal provisions (e.g. in national public law), direct intention can be established.

3. Informal information sources. If manufacturers or their representatives have said, expressed, or if it is stated in search systems through such mediums as tags that the software fulfils one of the purposes in Article 2(1), direct intention can also be established.

Secondarily, sources for discerning manufacturers indirect intention:

1. Data gathering practices. If the software gathers or measures data that is relevant for fulfilling the purposes in Article 2(1), an indirect intention can be established. This can be biometrical data about, as well as health records of, a natural person.

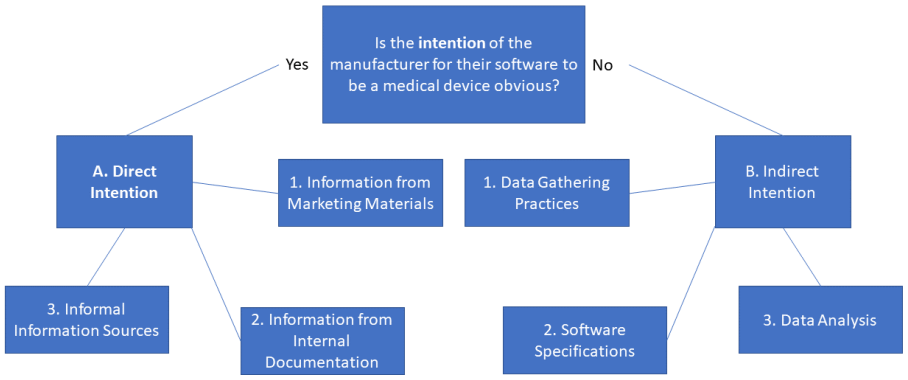
Common Legal Challenges" (2020) 4(1) Journal of Open Hardware 1.

2. Data analysis. If the software, as part of its purpose, requires personal data to be analysed to reach results that resemble or fulfil the purposes in Article 2(1), an indirect intention can be established.

3. Software specifications. If the software is designed and made to function as a medical device, either with the aim to substitute or replace existing MDs without being one itself, an indirect intention can be established.

This concept of a duality of intention can be illustrated, which is done below.

Figure 3.4: Figure of the Framework of Intention.



3.4.2 Safety Considerations

The legal arguments from above are one part of the background to proposed split between direct and indirect intention. The other is safety, which can be summarised in the following manner:

The safety capital of anything which is used in the same manner as a MD is immense; it can potentially psychologically or physically damage the user, but without there being practical and regulatory mechanisms to support the

patient. There will not be authorities who can be alerted to the harms the software or hardware can cause (and can withdraw the systems), health and normal insurance may not apply, and other kinds of administrative support may be impossible to make use of. While there are cases to be made about idiosyncratic medical devices (which are exempted from the MDR) or orphan medicine,[121] and situations where open source software and hardware solutions may be necessary,[122] the approval and release process should be smooth within the MDR, and not harm the patients and medical staff who need these resources.

This gives us a trade-off, where applying our proposed framework may increase safety and security but will always cost more time compared to having no regulation. Conversely, having no regulation leaves the users vulnerable, whereas having regulation is supposed to give guarantees both before and after an accident or harm has occurred. As the EU does not have competence to dictate how member states force their authorities and notified bodies to function, a guarantee for time between applying for one's product to become a medical device, and for the product to be released cannot be given.

[121] M Dooms, "Orphan medical devices have come a long way" (2023) 18(1) Orphanet Journal of Rare Diseases 71 ⟨https://ojrd.biomedcentral.com/articles/10.1186/s13023-023-02685-7⟩ accessed 10 October 2023; Melvin T and others, "Orphan Medical Devices and Pediatric Cardiology – What Interventionists in Europe Need to Know, and What Needs to be Done" (2023) 44(2) Pediatric Cardiology 271 ⟨https://link.springer.com/10.1007/s00246-022-03029-1⟩ accessed 10 October 2023.

[122] Mercedes J Burnside and others, "Open-Source Automated Insulin Delivery in Type 1 Diabetes" (2022) 387(10) New England Journal of Medicine 869 ⟨http://www.nejm.org/doi/10.1056/NEJMoa2203913⟩ accessed 30 April 2023; John W Lum and others, "A Real-World Prospective Study of the Safety and Effectiveness of the Loop Open Source Automated Insulin Delivery System" (2021) 23(5) Diabetes Technology & Therapeutics 367 ⟨https://www.liebertpub.com/doi/10.1089/dia.2020.0535⟩ accessed 30 April 2023.

3.5 Application of the Framework

This section focuses on how the direct/indirect intention framework can be applied to European regulation of medical devices. It does so through some cases, a discussion of what it does in a broader academic legal sense, and how it affects each party surrounding the MDs as subjects.

3.5.1 Cases

This small subsection provides a walk through on how both sides, direct and indirect intention, can be understood and used. It uses two examples, in the form of *wearables*, which can be interconnected with wellness and personal health apps,[123] and *chatbots*. First is used in both types of intention, and latter only in indirect.

Figure 3.4 initially divides intention up into direct and indirect. Wearables can fall under both categories. Chatbots, unless already certified as MDs, will be relegated to indirect.[124] We start with direct intention.

- 1. Direct Marketing Materials. Wearables are often sold to monitor, improve, or otherwise modify the health of an individual or groups. This constitutes directly communicating equivalence to what medical devices have to fulfil in Article 2(1) of the MDR.

This source should be the most common, and clearly illustrates what the manufacturer intends to do with their product. Wearables are often sold in

[123] Which is well-known and analysed without them legally necessarily being MDs, see e.g., Chiara Gallese, "Legal Issues of the Use of Chatbot Apps for Mental Health Support" in Alfonso González-Briones and others (eds), *Highlights in Practical Applications of Agents, Multi-Agent Systems, and Complex Systems Simulation. The PAAMS Collection* (Series Title: Communications in Computer and Information Science, Springer International Publishing 2022) vol 1678 ⟨https://link.springer.com/10.1007/978-3-031-18697-4_21⟩ accessed 25 June 2023.

[124] Whether they should, are, or will be, is part of a larger debate, ibid.

tandem with software, and the direct marketing materials for both can indicate their intention, through promises of improved health, self-surveillance, and other types of wellness optimisation. For specialised hardware and software, that intrinsically only focuses on one thing, like a specific diagnosis or area, the intention should also be well established.[125]

- 2. Information from Internal Documentation. This source for determining intention can only be used if the product is under investigation, through leaks, or otherwise, and would instead focus on direct admissions or statements which could be seen as fulfilling Article 2(1). Wearables could internally be strategically developed and aimed at partially or fully overtake existing MDs, which can be completely clear from this source.

Internal documentation tends to showcase the inner thoughts and ideas which are behind the product; this also means it can directly be used to infer intention. Wearables could be made to replace existing medical devices, such as classical blood pressure monitors, blood sugar measuring equipment, sleep measuring equipment, and so forth. Many types of measurements can be done through simpler means, and the internal documentation may convey this very clearly. The manufacturer could be interested in effectively bringing a more inaccurate and worse product on the market - to provide some of the same services as existing MDs without having the same production costs.[126] It could be conveyed in a more deceptive manner, which connects to the three types of indicators in indirect intention as I will mention below, where analysis viewable in the internal documentation clearly states elements which align direct with Article 2(1).

[125] A downside may be the situation where, if the manufacturer is careful, the materials can be written specifically enough to not clearly convey fulfilment of Article 2(1), and any of the other sources will be needed to do so. In those situations intention may be established through any of the other categories.

[126] But patients and even users may suffer because of this.

- 3. Informal Information Sources. This is included for completion, in case there exists additional documentation or other indications which the relevant authority can make use of to uncover clear intentions for the wearable to be a medical device. These can be found anywhere, whether unintentionally written internally (but not approved or part of systems in the company), or from elsewhere.

What makes this different from the second source, is that the text or other media is not part of the company's approved or deliberately procured external or internal documents. For wearables, this could be informal comments or other statements from employees, shared online or closed groups on various platforms, or statements heard and recorded in public, or personal notes on work devices or similar. This category primarily exists to cover all other types of literal or almost-literal statements or indications of intentions, which could be an admission of the system being capable or actively fulfilling Article 2(1), and these sources can be gathered by anyone, including interests groups, individuals, and so forth, and this being public could influence the authorities to further investigate and make use of the two sources above to fully unveil the intention.

We now move to indirect intention.

- 1. Data Gathering Practices. If wearables or chatbots directly and clearly gather data that would fall under what can be seen in Article 2(1), then this source can be used to illuminate whether there is an indirect intention for them to be MDs.

Gathering of data does not always have to be detected at software level; sometimes third parties, or even users or patients may notice it, and this can trigger further investigation.[127] This category acts strong as an indication, or a reason for further investigation, while the two below stand very

[127]Furthermore, chatbots, which are not certified and monitored, risk leaking all the

strongly on their own. Additionally, the practices can only be considered part of external or internal documentation above, an example of sources of both direct and indirect intention functioning together.

- 2. Software Specifications. If the technical design of the chatbots or wearables by itself reveals its nature of, e.g., attempts at profiling in the form of preliminary diagnosis of individuals, this may be enough to also constitute indirect intention.

Specifications are design tools or documents, which could also be filed under category 2 in direct intention. They have their own separate category here due to their technical nature, but in practice there will be some overlap. For chatbots, their design or means reveal what their creators intended for them to do. For wearables, further physical specifications (what can it physically measure) could also indicate intention.[128] But the latter is special, since it cannot stand on its own, as many devices measure common inputs also measured by MDs (such as heart rates), while not intending to be a medical device at all. This is clearly the case for wearables such as smartwatches which specialise in supporting physical activities like running. The gray area comes in the form of smartwatches which can measure that and more, and which actively have the potential to fulfil Article 2(1), and where the conundrum can only be revealed through specifications, and not from their actual analysis during deployment, which is the category below.

- 3. Data Analysis. If characteristics or elements of diagnosis, monitoring of health conditions or similar is done within the software in

assumed and potentially wrongful information they have gathered from patients to adversaries in the event of a successful attack. This is true for the other two categories as well.

[128]Note that the physical specifications still require software specifications to function, hence the category not being called "physical and software specifications".

chatbots or wearables, then this constitutes clear indirect intention for them to be MDs.[129]

Similar to above, it is the hidden actions or information which can reveal the intention. In chatbots, the processing, when finally revealed if hidden or in Black Box form, could hint at what the manufacturer really wants to do when the patient and/or user meets the system. If there is likelihood based analysis of categories of the subjects and types of sentences, or rates at which messages are being analysed, leading to profiling of the patient in potentially diagnosis-like boxes present when the system is deployed, then that hints at a strong indirect intention for the chatbot to be a MD. In wearables, innocent types of analysis initially could also be found to be a much clearer intention for their equipment and software to be MDs, if they, e.g., are actively aware of the issues with heart rates and clearly profile their user as a patient with a specific condition.[130] Sleep monitoring wearables, which analyse the data measured to improve sleep to assist the user, may also discover causes or direct reasons why their sleep is poor, which could potentially be through or more or less direct types of diagnosis. While this is positive, there is no reason why these types of software and hardware should not be considered medical devices, if they can lead to this outcome, in the same way that official equipment used in, e.g., specialised settings like epilepsy monitoring does.[131]

[129]For chatbots, it will mostly be text or sentence analysis, and this can primarily be aimed at psychiatric disorders or similar, not physical health conditions as such. This does not preclude Art 2(1).

[130]Or the opposite, the patient has informed the software that this is the case, but then the device would now be monitoring the condition, again at least in spirit fulfilling Art 2(1).

[131]Jen Sze Ong and others, "Medical Technology: A Systematic Review on Medical Devices Utilized forEpilepsy Prediction and Management" en (2022) 20(5) Current Neuropharmacology 950 ⟨https://www.eurekaselect.com/197799/article⟩ accessed 19 October 2024.

Summary of the cases:

Firstly, applying The Framework of Intention for Manufacturers of Medical Devices requires context and source of information. If this does not exist, then it cannot function, and the intention of the manufacturer can then not be discerned. Secondly, the framework only functions if there little doubt as to what the manufacturer communicates, if direct intention, or if there is little doubt as to the technical capabilities and functions in indirect intention. For wearables, as mentioned above, it must be made clear whether the equipment and software only measures and analyses healthcare related data, but without diagnosing or monitoring diseases or disabilities, or similar, as it would only be considered generic hardware or software if so. For chatbots, if not sold or otherwise clearly directly intended to be MDs, their technical specifications, use, or just gathering of data must indicate purposes or fulfilment of purposes that teleologically or actually fulfils Article 2(1) in the MDR. This leaves us with a theoretical framework which must be used carefully, and is in no way perfect, but which answers some of the complaints and issues which the medical device community may have.[132] The next subsection includes additional comments on the framework and its reason to exist in practice.

3.5.2 Regulatory Capture

Efficient and necessary regulation of products, especially regarding consumers and usage which can potentially harm patients or users, is always a goal of any type of safety regulation. But all types of product regulation have one weakness; regulatory capture.[133] Regulatory capture refers

[132]Stephen Gilbert and others, "Large language model AI chatbots require approval as medical devices" [2023] Nature Medicine ⟨https://www.nature.com/articles/s41591-023-02412-6⟩ accessed 10 October 2023.

[133]This is not to be confused with the idea of regulatory capture in Political Science.

to the notion that all necessary subjects are covered by the definitions and boundaries created by the legislation - this is specifically the issue which this framework addresses. Instead of letting direct intention be the only measure for regulatory capture for the MDR, this framework allows actual analysis of usage and hidden intention of the manufacturer, to designate when something is a medical devices, and when something is not. This is all done within existing legislation, by interpreting the wording teleologically (the spirit of the wording). Whether this is feasible in practice requires testing at the courts or at a national authority, but the cases above indicate the possibility. But this would solve some of the issues that product legislation often represents, which is specifically prudent for items which can severely harm individuals.

For Authorities

In our new framework, the role of the authorities is as central as ever. Direct intention is, by definition in the MDR, left to the manufacturers to show, but is also already considered by both notified bodies and national authorities. As such, this would remain unchanged, and their understanding and obligations would not literally diverge.

For indirection intention the situation is quite different. Authorities, with their powers of market surveillance, must expand this to include other types of software and hardware, which could potentially be medical devices based on their actual usage and construction. For software, this would be within what these authorities are already capable of; controlling and analysing applications in relevant online stores or being aware of what online communities currently use of free and open source software.[134] The issue lies in these powers, as they are usually not used at the

[134]See the paper on open source insulin delivery systems from earlier, Lum and others (n 122). The observations from this and other papers mentioned can be relevant to keep

initial stage, but instead further down the process of medical device certification - but national product authorities, especially in consumer situations, have and use their powers in this manner too. This would therefore be a natural expansion, even if not directly or literally asked for by the MDR. The process after identification, that is, where the authority designates the product as being a medical device, would be the same as with *direct intention*, meaning testing and design specifications being relayed to both the authority and the notified body, and the latter would then test the product as per usual procedure.

On balance, the framework would increase the burden on both authorities and notified bodies but would make use of principles which they both already use, and expertise which they should already possess.

For Manufacturers

It should be clear by now, that the framework would always increase the obligations of some manufacturers, though not those who already submitted or otherwise are clear about their products being MDs. Conversely, any who make systems which either by internal intention, such as decisions taken within the company or community, or from their design or usage in practice are MDs, would be considered medical device manufacturers if fulfilling the *indirect intention* requirement, as can also be seen above in the cases. For those who would not be covered by the MDR before, their obligations would go from zero to one hundred percent, and they would be burdened with additional tasks to fulfil. On the other hand, they would be provided with legitimacy and recognition, and make use of the support which national authorities and notified bodies are also supposed to provide. But it would clearly be a net cost for these, and for open

in mind.

source projects where no legal entity, centralised control, or similar measures exist, mandating these to follow the MDR would be akin to banning the product in the EU. The latter is an open problem which has not been resolved, although parallels to orphan medicine may be a solution in terms of guidance provided. Regardless of this, the MDR has nothing which could help these specific types of manufacturers further.

Role of Users and Patients

Before, the actual usage of medical devices did not matter to the MDR; authorities may in practice have taken notice of it but could chose not to. With the framework, this is turned around, and the actual usage of the devices, due to *indirect intention*, is now taken into consideration. If software is popular and widely used to self-diagnose psychiatric disorders, then it should be considered a MD, if large groups of people build open source insulin pumps or IoT biometric reading software, then it should be halted and certified (perhaps in collaboration with authorities) or banned depending on circumstances and so on. The impacts for users and patients are different, and yet also the same, as the three examples above show. For the two last, patients and users are the same, but for the first, while you may "use" the application to do something, you do not control or understand the MD, and can therefore only be considered a patient. Users are not empowered purely by our framework - they may potentially become pseudo-manufacturers, meaning increased obligations or bans of their used medical devices. Conversely, the safety and security of patients will be increased as these medical devices are certified and must fulfil general MDR rules and guidance.

3.6 Danish Law as a Case Study

In this section, it is shown how patients can use applicable law to recover their damages from an adversarial attack on a surgical robot in Danish Law, where the adversary cannot be identified.[135] The section also shows whether a lawsuit with product liability, reimbursement outside of contract or a case in the Patient Compensation system in Danish law will be likely to succeed, and it is done so from the perspective of the patient as the claimant and the manufacturer as the defendant. These means are analysed as they are the only way in which an injured individual could claim compensation from the damage caused on them, and because manufacturers of such robots must be aware of their liability and the following potential risks of litigation.

This section cannot literally apply the framework above, as this is a case study that uses Danish applied law, *de lege lata*, and the terms used can only be those seen in past case law and positive legislation. In the future, the framework could be used, but this has yet to happen, and the same goes for the use by authorities or courts.[136]

Initial comments

Robots or CPS as such in Danish law do not have *lex specialis* made for them, and outside the implementation of EU security legislation, security and adversarial attacks do not have any either.[137]

Before one makes use of the most general approach to compensation, two

[135] This is a common occurrence, and identifying and suing them would lead to simpler lawsuits, which is not within the scope of this chapter.

[136] The section is not an attempt to test the framework in practice, for a shorter analysis of how it could be used there, see the "Cases" section above.

[137] Directives are implemented into national law, not directly used like regulations, see Art 288 in the Consolidated Version of the Treaty on the Functioning of the European Union.

other types must be considered, as these are *lex specialis*, albeit not for adversarial attacks or security. One must therefore go through product liability,[138] then Patient Compensation Association below. Patient Compensation is not a lawsuit, but a separate administrative means to claim compensation.

However, both specialized approaches build on the thoughts from reimbursement outside of contract, a case law based means to receive compensation in civil litigation. This is not to be confused with extracontractual liability, which as a principle applies strictly to reimbursement at all times when there is no contract dictating the terms. In contrast, reimbursement outside of contract includes legal principles that are far older than the EU, which modify and set boundaries together with Danish contract law in general. Furthermore, extracontractual liability does not include the process and other rules regarding issues beyond liability, which reimbursement outside of contract always does. Because of its special role and much longer existence than the other two, a patient can always fall back on this. To sue on the basis of reimbursement outside of contract requires that 4 specific case law based criteria for reimbursement are fulfilled: *someone who is liable, quantifiable damage, a link between the responsible and the damage and that the link is adequate,*[139] and these must be fulfilled cumulatively. The defendant may have acted carelessly, and the adversarial failure may have caused damage, and a link between the two can be made likely, but if the link is not adequate, the case will be ruled in favour of the defendant. The last approach will come after the other two.

Both of the types of lawsuits will be part of civil litigation.

[138]Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L210/29. Danish implementation of the Product Liability Directive in Danish law is done through the Law of product liability, LBK nr. 261, 20/03/2007.

[139]Bo von Eyben and Helle Isager, *Lærebog i erstatningsret* (7th, Jurist- og økonomforbundets Forlag 2013) 23.

3.6.1 Product Liability

If a product is defective and causes damage, a lawsuit on the basis of product liability can be initiated. Defect is defined as the product being less safe than a person is entitled to expect.[140] Normally, this would not apply to a product (here a surgical robot) which has been purchased by someone else than the patient who was injured by it, but the following case allows this in Danish law.

If a patient being treated by a medical device that fails due to a defect and gets injured, the patient is entitled to directly sue the manufacturer instead of the hospital in Danish law. This was answered more than forty years ago in the case U.1960.576H,[141] where two patients kept the manufacturer of oxygen machines liable and had to compensate for the damage that was caused on them as they were hospitalized.

Product liability can be sought in three ways in Danish law. The first is on the basis of the product liability directive, the second is through a case law based approach that existed before the directive,[142] and the third is the oldest and is product liability through contract.

Product Liability Directive Lawsuit

Lawsuits for product liability are usually initiated on the basis of the Product Liability Directive as transposed in Danish law.[143]

First, it is seen that the surgical robot and accessories are included by the law, since it is a product.[144]

Secondly, one must consider whether the manufacturer is exempted from responsibility. Surgical robots that are not considered goods are exempted.

[140] See Art 1 in the Product Liability Directive, or § 5 in the implementation law.
[141] Notation for Danish case law.
[142] Also called "delict based product liability".
[143] Andersen and Lookofsky (n 123) 498.
[144] See § 3 of the implementation law.

This refers to idiosyncratic surgical robots that cannot be moved without destroying them.[145] The defendant can further argue that if the surgical robot has not been put into circulation, has been designed to be used by a single hospital, or that due to the state of the art the time it was impossible to discover the defect, they are not responsible.[146] The last factor is especially important since this enables the defendant to argue against any adversarial failures caused by new or unusual means, but the burden of proof for this is incredibly high, as it is the knowledge of the *entire industry*, not just what the single manufacturer knew at the time.[147] This then becomes a case of inviting the best expert witnesses or hoping that the claimant ignores new or extraordinary research.[148]

If the manufacturer is liable through this method, the rest of the process can follow. The claimant must then prove that a defect exists.[149] They also have to prove the damage and the link between the defect and the damage.[150]

A defect is defined as the product being less safe than a person is entitled to expect,[151] and the patient can claim that they can expect for the surgery to only fail due to mistakes by the operator or mechanical or safety failures, not those caused by adversaries. Three considerations can modify this assessment, the marketing of the product, its intended and expected use, and the time at which it was put into circulation.[152]

Marketing is irrelevant to the claimant, but intended and expected use will

[145] This also means they are not products because they have not been put into circulation.
[146] See § 7, part 1.
[147] This contrasts with the model that the MDR uses in state of the art.
[148] On the contrary, this may let medical devices related to orphan medicine to be exempted, though there is no case law that indicates it yet.
[149] See § 6.
[150] The criteria are partially derived from the aforementioned reimbursement outside of contract.
[151] See § 5.
[152] See § 5, part 1. This is similar to the Framework of Intention, specifically for direct intention, which was created above.

include some unusual considerations when it comes to the last exemption in § 7, part 1, 4 or part 2, which is "consequences that could not be foreseen at the time of sale". Since the use of such a robot naturally will include maintenance of any level of software, evading responsibility is impossible on those grounds when considering security aspects, unless it is impossible to defend against, such as future adversarial failures caused by quantum computing. The exception will only apply to extraordinary adversarial attacks, as zero-day attacks and exploits are not unforeseeable and will always have a chance of occurring.[153]

Identifying the defect is crucial, which would require that the claimant obtains proof of the three adversarial failures that potentially can cause an injury on the patient. These are manipulation attacks, subversion of robotic control and poisoning of the feedback loop, which was discussed earlier in this chapter. The claimant can then require original design documentation, which an expert witness could question as to whether the surgical robot is under the risk of specific manipulation of the robot or subversion of the control of the robot over the network, as well as poisoning of the feedback loop given from visual and haptic sources.

Another approach, which is even more appropriate, is the argument *res ipse loquitur*, proving that the injury was not caused by human or other error. This will force the defendant to either argue that it was caused by a safety defect, which will make no difference for the injured party other than a new lawsuit, or make the defendant argue why the failure had not happened. The claimant can then claim that since it could never be caused by human error or a safety defect, it must have been a defect that the defendant is responsible for. As this is a civil lawsuit, in the situation where the defendant decides to deny all claims and not argue the claimant is likely to

[153]Though some defences can still be made, see e.g., Halperin and others (n 169).

succeed, as silence on the matter speaks against the defendant considering the severity of the damage. This is further supported by the role this and reimbursement outside of contract lawsuits present, since they will be used in situations without insurance.[154]

The claimant will then have to prove the damage had occurred, which one can assume that they are able to, but they also have to prove the link between the defect and the injury.

The claimant can choose to argue for a *direct* or *indirect* link. For the link to be direct, it has to be physically seen or decipherable from log files. For it to be indirect, it has to be derivable from the situation. There are two cases that illustrate the duality of the indirect link. Lawsuits from the case law based approach are free to be used in the directive based approach, even if the legal sources for it are different.

In the case U.1939.16H, cattle owned by the claimant died after being fed black treacle. Out of a set amount of cattle, only those fed with the black treacle produced by the defendant died the following week. The claimant claimed, after having used an expert witness that showed that they were in good health before being poisoned, that they had not been overfed or otherwise damaged by the claimant, that the cattle which were not fed with it survived, and that poisoning from the black treacle could therefore be the only cause of death. The argument was built so because a vet at the time could not clinically prove it, which is why the link is indirect. Black treacle acts as supplement and is not supposed to have any drawbacks. The defendant argued that the claimant had not proven this sufficiently but did not provide additional reasoning for why this was so. The Danish Supreme Court found that there could be no other reason for the deaths and sided with the claimant.

[154]Considerations on insurance are not included, as this is subject to contract and is specific for each company that provides it in Danish law.

In the case U.2003.1706H, the claimant's roses that were fed with peat manufactured by the defendant experienced distorted growth. The parties agreed that the distorted growth was caused by oxygen deprivation. An expert witness brought by the defendant made it clear that the contents of the peat were fit for use. The claimant used the same argumentation as from above, that is, that due to the circumstances, the peat causing it was the only plausible outcome. The Supreme Court found that just because the distorted growth stopped after a change in peat did not mean that the peat was the cause, nor that the peat could have been different than how it was described, and that the peat was not different than what was previously agreed and delivered between the parties. The court therefore sided with the defendant.

If case law is applied, it can be seen that unless the claimant has access to log files that show adversarial failure, or design documentation that shows which defences and adversarial failures that were considered, the claimant should try to argue for an indirect link. They are likely to succeed, since the concept of the same product suddenly having a defect, the argument from the second case, does not apply to adversarial failures that are caused by inadequate defences. This is because defences are created to defend against threats, and requiring maintenance and updates is usually part of the service agreement on purchase.[155]

The defendant has a case law based tool they can make use of, which is the test for whether the defect is "systemic damage",[156] which if true, shows that the product cannot be considered defective. The distinction between danger and defect is explained below but has no effect on the test. The defendant would have to build their procedure around the test being

[155] However, if such an agreement is not part of the purchase of the surgical robot, the claimant will likely not be able to establish an indirect link.

[156] Andersen and Lookofsky (n 123) 477.

fulfilled, which equates to two questions that must be answered with a yes. These are:

- *Are the dangers known?* The danger of manipulation attacks, subversion of robotic control and poisoning of the feedback are all known, but they are not necessarily known for each type of surgical robot. It has been known for the product. The claimant can argue that they are not known and ask for documentation for this otherwise. The defendant can retort that the underlying risk of any type of adversarial attack equates to public knowledge of the dangers. But the defendant is unlikely to prove anything with such a general argument, since it is product specific, which is known from e.g., U.2015.572H[157] that "known" refers to the product only, and vague statements are not accepted by the judges.

- *Are the dangers unavoidable?* Unavoidable refers to whether the scientific and technical community deems it to be likely. The defendant can claim that all adversarial failures are generally unavoidable because of new techniques and vulnerabilities, which is an argument of constant development. The claimant would retort that certain adversarial failures are more preventable than others. The exception would generally be subversion of robotic control, because the manufacturer cannot perfectly control the network that the surgical robot receives commands over.[158] They are however able to build suitable defences against the rest, even if doing so in CPS is difficult.

It is unlikely that both questions in this test can be answered with yes,

[157] A groundbreaking case, where a claimant tried to sue the manufacturer of a big tobacco brand for the cancer that the excessive use of cigarettes had caused. They failed, because the damage caused to the claimant was considered systemic, because it was both known by everyone concerning the product, and unavoidable if you smoked it.

[158] This responsibility is incumbent on the hospital or any subcontractors that maintain networks and IT infrastructure.

since the public at large does not know that these adversarial failures can occur to surgical robots, but certain adversarial failures may be considered unavoidable. Most importantly, the judges have to be convinced of this, and even if both could be answered positively, that does not mean that the judges will decide to allow the test.

Product liability Lawsuit via Case Law

Initially, it has to be mentioned that EJEU has concluded that this approach can only be used where the product liability directive does not apply,[159] where a Spanish set of product liability rules that put the patient/consumers in a more favourable position was ruled to violate the directive.[160] This approach can only be used on surgical robots that are not covered by the directive.[161] In practice this would limit it to completely custom made surgical robots, as well as those that cannot be moved without being destroyed,[162] and MDs made for orphan medicine with little to no distribution, unlike the directive based approach.

While the test of systemic damage, and the use of case law from earlier, still apply to this approach, there are certain differences in how the defect is defined. Both the definition of defect from above can be used, as well as the old term "danger".[163] If the product can injure the user or third person, it is considered dangerous. But to be defective, it has to be "unreasonably dangerous".

This implies that some products are inherently dangerous to use, but it is the manner of danger outside of this that determine it. Candy as an analogy is not unreasonably dangerous, but excessive consumption may

[159] See e.g., case C-183/00 *González Sánchez* [2002] ECR 255.

[160] Andersen and Lookofsky (n 123) 471.

[161] See § 3 from the law of product liability.

[162] However, if EU law or the system ever changes, one can revert to relying on this case law based approach.

[163] Andersen and Lookofsky (n 123) 476.

increase weight and damage health of individuals. Any software system or device that is connected to the internet or local network poses a direct danger to the patient due to the known vulnerabilities and possibilities of abuse it contains. But for it to be unreasonable, it has to have a risk that occurs often or commonly, which so far seems not to be the case here.

The use of defect from the directive is therefore appropriate, since unreasonably danger would likely not cover adversarial failures, and because the terms can be used interchangeably in both approaches.

Otherwise, the case would proceed as above.

Lawsuit on Product Liability in Contract Based on Case Law

The contractual approach is next, which is included for the sake of completeness. It was created from case law, and has no legislation directly associated with it. If possible, this type of lawsuit would completely circumvent the rules laid out above, and instead merely focus on analogies to the Danish law of purchases, which would lead to cases where the evaluation of the sale of a proper product was met or not. This would apply to the patient as a third party and allow a lawsuit. To make use of this, the claimant must first prove that there exists a contract between them and the operator or manufacturer. The patient has not signed anything with either in written form, but it can be questioned whether the patient has done so orally. To assume the patient has accepted an oral contract with the hospital or the doctor, there has to be a so called "meeting of the minds"[164] in Danish law. Such a meeting must here include the acceptance of treatment being done in part or partially by a surgical robot, and the general risk of failure of the machine or anaesthetics. Whether they have to disclose the risk of adversarial failures is unlikely, since there has not been any such

[164]Gomard, Godsk Pedersen, and Ørgaard (n 69) 21.

failure publicly recorded in Denmark. However, the claimant is not likely to prove that this exists, since Danish healthcare law does not work with contracts between these two parties in the context of private law. This means that the judge would dismiss the case on the basis of a lack of a contract.

3.6.2 Reimbursement

The default for seeking compensation in Danish law is reimbursement outside of law, where the four requirements, *liability* (through acts of carelessness), *quantifiable damage*, *a link* between the responsible and the damage and that the link is *adequate*, have to be fulfilled.[165] Unlike the examples above, there is no objective responsibility, only *culpa*[166] which the manufacturer must have committed.

Traditionally the standard for what is not careless is what a *bonus familias pater* would do. This is criticized in Danish law,[167] and the standard is gradually moving towards a focus on the breach of rules (both legal and otherwise) or the "normal right to act". This is defined or at least elaborated on in case law,[168] but it has not specifically been done for manufacturers of CPS or surgical robots, nor for adversarial attacks in general.

Fulfilment of Criteria

For the lawsuit to be successful, the patient that was injured by a surgical because of an adversarial failure has to make it likely for the court to find the criteria mentioned earlier fulfilled. The defendant will attempt to disprove this in various ways.

[165]Eyben and Isager (n 139) 23.
[166]Can be understood as carelessness.
[167]Eyben and Isager (n 139) 87.
[168]ibid 85 - 88.

First, the claimant has to show that the defendant acted carelessly in relation to the adversarial failure. Like mentioned earlier, there does not exist *lex specialis* they can have broken here, such as notions of security and safety in the MDR, which would normally be enough to show carelessness.

The claimant will not initially have any documentation concerning what considerations were taken about the prevention of adversarial failures in the company. But they can bring forth the argument that the manufacturer failed to act to prevent the adversarial failure from occurring. This assumes this was made clear first, and if not, the claimant can say the same about the safety aspect that allowed the patient to be injured. The evaluation of carelessness is broad,[169] so the claimant could also bring out the danger of a surgical robot, which by its very nature warrants the utmost caution in both its design and later service. The defendant can either choose to bring out the documentation which shows that they did consider the one adversarial failure that caused the injury but could also go for the approach where they do not reveal which one. Like in product liability, this is a disadvantage since silence or dismissal does not by itself prove anything in a civil lawsuit, unless the claims are unreasonable or out of proportion.

Due to the severity of the injury and of the significant risk it poses, as both the da Vinci and Magellan systems can cause internal haemorrhage, the barrier for carelessness is further lowered. The final nail in the coffin would be the support of "responsibility based on profession" that is seen

[169]ibid 122.

in case law[170] regarding safety in this area.[171]

In a security context, it can be argued that if it is known that manipulation attacks, subversion of robotic control and poisoning of the feedback loop is possible, any professional (here manufacturers) must make all attempts to mitigate it and must prove they have done so to not be held liable. The claimant is therefore likely to be able to fulfil this criteria.

A clear way to show carelessness is if rules have been violated or otherwise not complied with.[172] Even if the case is not about personal data, if the defendant had breached GDPR,[173] the bar for proving what is mentioned is further lowered, but not as clear compared to if *lex specialis* was breached.[174] On the other hand, the defendant could bring out the argument that a third party (like the hospital) had not complied with security legislation such as the NIS1 or NIS2 directive, which would enable the defendant to prove, that if the breach of security by the hospital caused the adversarial failure or made it much more likely, they would not be liable. If this were the case, such a lawsuit would require the claimant, after having lost the initial lawsuit against the manufacturer, to sue the operator (hospital) of the surgical robot instead.

Finally, the claimant could make use of the idea that the defendant had broken the rules of "state of the art" security, which is found in Annex I

[170]To illustrate this tightening of the evaluation of culpa, U.2010.1350H is used. In the case, the defendant had installed ventilation equipment at the address of the claimant, but a fire developed after the defendant had left the property. This had happened due to a known defect with smoke cartridges after the installation, and the defendant knew this from their own experience and otherwise. The judge concluded that because of this knowledge and because they are considered professionals in the business, they acted carelessly and were therefore responsible.

[171]Eyben and Isager (n 139) 12.

[172]ibid 89 - 97.

[173]Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[174]There exists specialised legislation on reimbursement in specific situations in Danish law.

of the MDR. This would then entail a similar analysis as to what constitutes, and what does not constitute this type of security, but it remains an additional option, though it would require substantial expert witnesses and similarly convincing technical evidence; it would be wiser to make use of the other means above.

It is assumed that any injury sustained is quantifiable, which means that the second criterion is fulfilled. The claimant would need reports from hospital staff and could also get a second opinion on the injury. This will be contested by the defendant, who might bring an expert witness to scrutinize the documentation provided by the claimant.

The next issue becomes whether there is a link between the careless behaviour and the injury. The claimant has to prove that the careless behaviour directly or indirectly likely caused the damage, and this is usually the most difficult part for the claimant to prove in a lawsuit. In reimbursement outside of contract, the claimant merely has to make it more than likely that the carelessness caused the damage.

The defendant can attempt to prove that the injury would have occurred no matter what they had done, which brings us back to the different adversarial failures. If the failure is subversion of robotic control, there are situations where the manufacturer could not have implemented defences that could have prevented or mitigated it. In that situation, it would only be the network administrator and therefore the hospital that could have prevented it, which makes the lawsuit unlikely to succeed. But in regard to the other two, the claimant can argue that the chance of the adversarial failure occurring would have been lower had the defendant actively attempted to prevent it.

The defendant can retort that the injury would have occurred regardless of their behaviour. This is related to the idea of *conditio sine qua non*, where

the act of carelessness must have made it more than likely for the injury to occur. To do this, they would have to prove that the adversarial failure was impossible to prevent or mitigate, therefore making the link impossible to prove for the claimant. The burden of proof is also comparatively high and would likely only apply to subversion of robotic control.

The defendant can highlight a tangential issue regarding the link, which is whether there are competing causes for the damage. They can argue that there always exists a risk for an adversary to cause an adversarial failure, regardless of their mistake, for example caused by the failure of software vulnerabilities in generic operating systems on their devices. But the defendant would again need to prove this, and vague general statements about "technical advancements" and "new techniques" from hackers are too vague, and it can be argued that they do not constitute a competing cause.[175] Even if they can prove that an update of software, they do control caused the failure, this does not equate to the judge supporting the argument, nor does it refute the compelling argument made by the claimant. In fact, this likely undermines their case, as they as the professionals must be able to handle updates to proprietary software that works in their manufactured equipment. This area may change since CPS consists of many types of software constantly working together, and if adversaries abuse known vulnerabilities in proprietary OS or the like, to make a surgical robot suffer an adversarial failure, it may constitute a competing cause that could disprove the link between liability and damage. But the small line between disclaiming all responsibility for choices they themselves take (using software they have not developed in their own robot) and taking it is thin.

A piece of safety case law can further show how difficult proving the link

[175]This is because the vague statement is part of the background of the causes, as security as a branch accepts the risk of new developments, see Eyben and Isager (n 139) 313.

can be.

In the case U.2011.354Ø, the ship of the defendant was captured by Somalian pirates. The claimants, the employees of the ship, claimed that the captain had not established increased surveillance of the dangerous waters, and had not taught the crew to use the alarms designed for these situation. The judge agreed, but found the defendant to not be liable, even if they had acted carelessly, since the capture would have occurred regardless.

If one applies this to this situation, it can be used by the defendant if they can prove, that the adversarial failures would have happened regardless of their careless behaviour. The analogy from pirates to adversaries is adequate but requires that the defendant must reveal all details that could show that the adversarial attack was overwhelming enough to warrant them not being liable. This will in turn reveal which defences the defendant has deployed, which the claimant can use in other ways with expert witnesses, which makes this tactic risky.

Overall, if the adversarial failure was caused inside the surgical robot (and not via subversion of robotic control), the link between liability and the injury is likely to be proven in court, since a third party (the hospital) possesses local data that can likely show the failure or if the defendant reveals it as part of the process, or due to an indirect proof of it akin to the two examples of case law earlier.

The last criterion is adequacy. Is it adequate that the link between the careless behaviour and the damage exists? This question is usually answered by case law, but adversarial attacks on surgical robots has not been considered by the Danish or Nordic courts yet. The claimant can argue that because the defendant is a professional party, with objective liability and a special role in both the product liability directive and the MDR, and be-

cause the harm is bodily, that the link is more adequate than not.[176] The defendant can then argue that they should not be responsible for any kind of attack directed at their produced machines, and that this should fall on the end user. Even if the defendant has contractually tried to abstain from any liability, this does remove the fact they are the only party capable of effectively preventing some of the adversarial failures, which would lead to the judge most likely dismissing the argument and contractual clause. The actions of third parties have been heavily discussed in the literature,[177] and it is clear that if a third party, such as the operator, caused the adversarial failure to occur by their actions, the defendant cannot be held liable. But situations where the action just made it more likely (and not guaranteed) does not mean that the defendant is off the hook. They must disprove this, easiest done with expert witnesses or compelling documentation that could e.g., show why the network security levels of the hospital were inadequate. With a very high burden of proof, the patient can prove that the manufacturer acted carelessly in certain situations and therefore is liable, they can definitely show that an injury occurred, they can likely establish a link between their injury and the carelessness, albeit only some of the time, and that it is likely that it is adequate. This makes such a lawsuit realistic, but perhaps unnecessary due to the option below.

3.6.3 Patient Compensation Association

Instead of a lawsuit, the injured patient can choose to apply online for reimbursement for the damages caused to their body by an adversarial attack on a surgical robot. The act of complaint and reimbursement access in the health-sector[178] defines the structure and the requirements for Patient

[176] Eyben and Isager (n 139) 302.
[177] ibid 302.
[178] LBK nr. 995, 14/06/2018.

Compensation Association and cases processed by it.

The Patient Compensation Association is a public authority, and filing a case means that they will gather evidence and evaluate whether compensation is to be paid. It is according to the same standards as the lawsuits, but because the Association can both gather technical documentation from other authorities and testimonies from surgeons and log files from the surgical robot, the most important documentation is the proof that damage occurred. This is also because compensation should be paid regardless of why the surgical robot suffered a failure (adversarial or not), as all that has to occur is for the robot to fail.[179] This is by far the safest and quickest way to receive compensation, and because of the argument above, it disregards any security issues and instead makes it about safety - which severely reduces any theoretical burden of proof that the patient may have had in regards adversarial attacks in the lawsuits.

The means to do so is called "Patient Compensation", which is not a lawsuit, but instead an administrative process to receive compensation. This is facilitated by the Patient Compensation Association,[180] which is financed and run by the Danish state and private parties,[181] and it solely considers and decides on cases in regards to patient injury.[182] It does so in the manner as any public authority would, via the principle of officiality[183] in Danish public law. This principle includes the collection of evidence by the authority if necessary, and perfect application of existing law and committing to the correct decision.[184]

[179] See § 20 of the Act.

[180] Staff includes doctors and lawyers.

[181] Such as private hospitals.

[182] See §§ 32 and 33 in the act.

[183] This principle is not codified, but seen in case law, literature, and Danish Ombudsman's practice.

[184] See the currently accepted definition by the Danish Parliamentarian Ombudsman <https://www.ombudsmanden.dk/myndighedsguiden/generel-forvaltningsret/officialprincippet/>, last accessed 11 December 2024.

The patient applies for Patient Compensation on the association's website. This means that in this case, the only parties are the patient and the state, since the subject of such cases can only be the one who initiates it, and the state is by default the one who compensates. This means that this way to receive compensation completely excludes the manufacturer and costs them nothing.[185]

The objective liability for this damage rest on the Regions that run the hospitals, which in practice means the state.[186]

The types of damages that are considered are laid out in § 20, part 1. Since it is not caused by the operator in our case, the damage sustained has to be caused by "errors or failures in technical apparatus". Any type of failure, whether it was caused by neglect or other, are considered to be covered by this type of damage. The damage has to be caused most likely by the failure or neglect, see § 20 part 1. This is especially important, when the patient was considerably weakened, and the injury likely would not have caused any damage had they not been sick. The patient is advised to make sure, that the evidence necessary to prove that the surgical robot failed is seen by the authority.

An adversarial failure in these kinds of systems is possible, and an injury caused by it always establishes a link between the failure and the injury. This style of link is not unlike the one from the past section or the next, but still has its own case law, which shows how it is defined.[187] But if the adversary is able to hide those details, the operator can still attest that

[185] If the manufacturers of surgical robots were also included as "private parties" and contributed to the Patient Compensation scheme, this would make Patient Compensation affect the manufacturer as well. This has been impossible to confirm.

[186] See § 29 of the Act.

[187] E.g., U.2011.1019H, where the death of a female patient, claimed to be caused by treatment with a bladder catheter at a hospital, was deemed unlikely because of the amount of diseases she already suffered from, which severely decreased her health. The lack of a link between the death and the specific treatment led to the dismissal by the Supreme Court.

the machine failed, so it would then go from a security to a safety case, of which there is well established practice that supports the patient, as well as the literal reading of § 20, part 1. This essentially means that the patient has two ways to prove § 20.

After the application has been sent, the authority will collect information from the hospital where the injury took place, including documentation created by the operator of the surgical robot. The patient is free to provide further evidence, but since the authority has responsibility to make the right decision, they do not need to. If they want to, the patient is able to access[188] which documentation the authority base their decision on and halt the process until they have provided further proof.

The decision can be appealed to the courts, or to the appeal board driven by the appropriate ministry.[189]

The amount one is able to recover is comparable to a successful lawsuit, but the amount can be larger as there are no court or registration fees. Only compensation for quantifiable damage and pain and suffering is possible, as the Danish definition of tort is not directly applicable here.[190] If the patient accepts the judgement, and does not act further, they will receive the compensation at the date of the decision.

In short, as long as the patient sustained quantifiable damage, and the surgical robot has sustained a failure, *even if it cannot be proven to have been caused by an adversarial event*, they are able to receive compensation.

The caveat to this is the situation where adversarial failures become commonplace. This could lead to a Patient Compensation case not being possible,[191] either because of a change in the act, or because the administrative

[188] Equivalent to a Freedom of Information Request, or other national tools.

[189] Relevant ministerial organ, usually under the Minister of Health, but each government decides their own structure.

[190] See § 26 of the Law of Reimbursement Responsibility, LBK nr 1070 af 24/08/2018.

[191] As it relies on the failure and unusual circumstances, and in reality, political willingness to compensate for the injures. This will hopefully never be the case.

practice would be interpreted differently.[192]

3.7 Adversarial Attacks in Civil Litigation

In this section an overview of themes from the Danish case is given, and this ties into how adversarial attacks on MDs connects to cybersecurity in court.

3.7.1 Adversarial Considerations

Different adversaries come with their own issues. Some may be so strong that their attacks amount impossible to defend against, and some give new opportunities for easing the burden of proof for the claimant or patient.
Terrorist organizations, nation states, cybercriminals and organized criminal groups all require additional considerations. If the adversarial failures are induced by parties who are covered by criminal legislation, here terrorists, cybercriminals and organized criminal groups, the cases would be different in practice. The police and prosecutors would collect evidence, which would make the burden of proof for both patient and manufacturer considerably lighter, since reimbursement and product liability cases can make use of the evidence collected in criminal cases. Additionally, if organized criminals induced the failure(s), additional resources would be delegated to the investigation, and the potential punishments would be higher. Same goes for terrorists since they are covered by anti-terror legislation.
Both they and nation states as adversaries can cause *force majeure*. This term in Danish law covers very unusual situations, where normal practice may not apply, which means the manufacturer is likely to not be kept liable. Stuxnet-like[193] malware can be a concrete example of sophisticated

[192] Such as assuming that adversarial failures would not qualify.
[193] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier* (techspace

malware, that in practice would lead to situations where *force majeure* would be called by the defendant. The aforementioned malware is an example of an attack that led to all our mentioned adversarial failures, at once, and similar overwhelming attacks from nation states cannot reasonably be expected to be defended against.

Acts of terror carry a similar connotation, and it would most likely lead to *force majeure* situations, unless the attacks were simple and easily preventable.

A cybercriminal causing a failure is one thing, but a named terrorist organization causing it is completely different to a judge. The number of resources available to prosecute organized criminal groups is higher as well, since they too have special legislation imposed upon them, which might also lead to a lighter burden of proof for the patient.

These exceptional circumstance exceptions exist in other jurisdictions under different names, and may have similar adversarial specific implications, as do *lex specialis* for specific adversaries.

3.7.2 Considerations of Failures

Earlier, 6 different adversarial failures that uniquely fit surgical robots were described. This can be divided into 2 broad categories regarding where they hit - internally and externally. Manipulation, reprogramming, misappropriation of trade secrets,[194] poisoning the feedback loop and software vulnerabilities all exist inside the surgical robot. Subversion of robotic control is external, as this is an adversarial failure which occurs via the communication channel of the robot. This has legal consequences, as this becomes the hardest adversarial failure to defend against and can therefore

rep, 1.4, Symantec 2011).

[194] Misappropriation of trade secrets is an adversarial failure, because the adversary is able to compromise data and compromises the defences of the surgical robot - regardless if the action has no consequences in the short term.

lead to litigation that will be ruled in favour of the manufacturer. This is because the standard of what can reasonably be expected from a manufacturer, or from medical devices specifically, does not stretch to controlling the communication channels, but merely the security of the surgical robot. It has to function as expected, and suffering adversarial or non-adversarial failures amounts to the opposite - within reason as subversion of robotic control causes these failures but must be mitigated by the hospital or anyone else controlling the network which the surgical robot uses.

3.7.3 Evidence

As expressed above, proving that the defect exists in the product, and whether the link exists between the defect and the injury are complicated for the claimant. Initially, they do not possess the necessary design documentation or files, which show that the adversarial failure caused their injury. Like in other cases, they can show that nothing else could have caused the failure, such as via expert witnesses or even the operators that worked with the robot at the time, or system admins. This would force the defendant to provide some of documentation directly or otherwise leave the claimant unopposed.

The MDR has a special function in regard to proofs in these cases. In Art 10(14), paragraph 3, if the regulator determines damaged occurred, it can upon request transfer of all documentation that it has access to the patient or their representatives, requiring there to be a public interest in disclosure to overrule any violation of data protection rights and without violating intellectual property rights.

But since civil lawsuits in Danish law can be held behind closed doors, documentation that in an open case would violate those rights can be used if deemed possible by the regulator. The court decides on whether it is

appropriate, if contested by the defendant. Public interest refers to what it literally reads as,[195] which means that it has to potentially affect more than the claimant, or have consequences otherwise, which adversarial failures on surgical robots likely warrant.

Proving the injury and the adversarial failure occurred in the Patient Compensation environment is different, as seen with the influence of public law and the lack of court rules. The full burden of proof does not lie on the patient, but on the authority. Since they merely need to decide on whether equipment encountered an error or failed, seeing the failure and damage occur would be sufficient. It is unknown whether they have individuals educated to read the logs that such adversarial failures will create, but they can require the hospital and/or manufacturer to explain this to them. Cooperation with the appropriate national regulatory agency[196] is possible as well, since the sharing of documentation between such parties is allowed, through the principle of officiality from earlier, as it includes gathering any information necessary and possible, and other specialised rules for sharing information between public authorities subject to the GDPR.

Like before, the most difficult parts of these lawsuits are proving the existence of the failure and whether the manufacturer is responsible.

It is known that the judges are willing to reverse the burden of proof, especially when they feel like they have a very low chance of uncovering the "hidden proof".[197] This refers to situations where the actors that cause the damage are wholly owned and used by the other party, which the claimant would have no way of understanding or proving anything about.[198] This is also called "the presumption of responsibility", and it leads to a situation

[195] See Art 10(14), paragraph 3 of the MDR.

[196] The Danish Medicines Agency in this case.

[197] Eyben and Isager (n 139) 169.

[198] This will always be the case regarding medical equipment in general; the patient should not have access or control over them.

where, if the defendant cannot prove that they did not act carelessly, they will be considered liable.[199] To reach this, the claimant must encourage the idea in the mind of the judge, that the necessary documentation they need will never come out of the defendant unless they make use of this principle.[200] But this is rarely used, and since it was shown above that the case can most likely be decided without reversing the burden of proof, it is unlikely. But the claimant should use it in the situation where the case would fail on proving the link, since the reversal will require the defendant to prove they did not act carelessly, which is difficult under most circumstances.

The courts can also choose to tighten the evaluation of carelessness, or assume responsibility to be objective because of the circumstances, with a central case for this being U.1957.109H. In it, a 14-year-old girl dropped out from an amusement park ride and got injured. She did so because the back of the seat in the ride failed, and as she did not cause unusual strain to the seat, the Supreme Court concluded that the park was to cover her damages, since the seat was not strong enough for the task is was made for, and the park could not disprove this. While the judges at the time did not call it tightening of the evaluation of carelessness, it is later seen as such.

This can be used by a claimant to argue that if the surgical robot and the infrastructure around it allow attacks that can cause bodily harm, they are not secure enough for their usage.[201]

If this argumentation is accepted, it allows the patient not to use resources to prove the liability.

[199] Eyben and Isager (n 139) 168.
[200] ibid 169.
[201] But the distinction between what the manufacturer is expected to be able to defend against, is still apparent here.

3.8 Future Work

Surgical robots are always at the risk of suffering an adversarial failure. Your surgeon will not make mistakes because they were hacked, but a surgical robot operating on you will. For the best interests of the patient, and within or outside the opportunities of the MDR,[202] taking the best practice from the Danish legal system would be advantageous on an international scale. A sort of Patient Compensation system implementation everywhere where surgical robots are widely used.[203] One can reduce costs for the individual, reduce costs for the manufacturer and streamline the legal process and ease the means of redress for the patient. The clear disadvantages are that the reimbursement amount could theoretically be lower than that gained from lawsuits, but this can be solved by legislatively forcing the proposed system (like the Danish one) to use the same legal principles to calculate costs. Another interesting feature is the blatant disregard of technology - what matters is that the machine failed, adversary or not. This makes it a safe technology neutral approach to an otherwise very technology specific problem and acknowledges the shift from safety to security problems.[204] It also removes most issues with burden of proof that the patient would have had, had they taken their cases to court.

The chapter also shows how product legislation is not a solved problem; the use of intent is seen all over this type of regulation, and the safety arguments used here could inspire ideas elsewhere. More work on this would be useful, as would a stronger focus on accessories. The latter especially

[202] See Art 10(16).

[203] Increased and clearer rights regarding the special situation that robotics in general put us in are supported academically, see e.g., Ronald Leenes and others, "Regulatory challenges of robotics: Some guidelines for addressing legal and ethical issues" (2017) 9(1) Law, Innovation and Technology 1 (Publisher: Taylor & Francis) ⟨https://doi.org/10.1080/17579961.2017.1304921⟩, 30 - 33.

[204] Note that many jurisdictions' use of tort law/reimbursement law already disregard technology, but that this may not be to the advantage of claimants or patients.

due to their role in the supply chain of cybersecurity, but also because they are all entry-points into the greater digital hospital system (if digital and not analogue).

Finally, further research into how cybersecurity can be thought directly into the regulation of digital devices at large should be done. Standards, guidance, and even case law is not as useful as positive legislation to increase the safety and security of society at large.

3.9 Conclusion

In this chapter, six distinct adversarial failures for surgical robots were initially created, to conceptualise and define which types of failures they may suffer from an adversarial attack, alongside five for non-adversarial failures. The 6 adversarial failures are: Manipulation attacks, subversion of robotic control, reprogramming of the robot, misappropriation of trade secrets, poisoning of the feedback loop and software vulnerabilities.

It was then shown how the MDR assigns liabilities and rights to both manufacturers of surgical robots and regulators. On the basis of this, a framework of intention was created, which allows the intention of the manufacturer to be both direct and indirect. This was then analysed how it may function in practice was illustrated, with consequences for each actor in the MDR.

Following this, it was shown how a manufacturer of a surgical robot could be kept liable for the damage caused to a patient by an adversarial attack in Danish law, through two types of lawsuits and a public law controlled non-court process.

The chapter answered the questions posed in the introduction in the following way:[205]

[205] "How can this legal concept be understood in cybersecurity", and "how can these

Medical devices, as a legal concept in cybersecurity, represent cyberphysical systems, but also insecurity, and is a central challenge that a modern digital society must be constantly vigilant about. This is partially because the consequences of failing security obligations can cause safety implications in the form of injuries or other types of damage to patients, but also simply because the devices can be unusable without it. Since the chapter highlights basics in cybersecurity, and then connects it to the direct requirements found in medical device regulation as such, it creates a picture of medical devices as understood through their role in hospitals and on their use on humans in general, where cybersecurity must play its increasingly larger role in keeping it safe and secure, and due to its new role in compliance. This twofold nature of the relationship between the legal concept of medical devices and cybersecurity, the inherent goal of security being increased and its new central compliance role, can be seen in other contexts where the security of cyberphysical systems has gained legal status, while also guaranteeing distribution of responsibility for when the parties must take their issues to court.

Cybersecurity of medical devices present unique problems posed by complex cyberphysical structures that the law considers in the light of functionality, standards, positive obligations, and collaboration between authorities. Law in this way views medical devices in a security concept context as product regulation, which is clear from the sources analysed in the chapter, but also in a very intimate way due to how normal security and cybersecurity directly affects all types of law. This is then represented in the variety[206] and role of the authorities, which in turn also illustrates how diversified law views security in medical devices. Because of its place-

cybersecurity considerations be understood in law"?

[206]Of which I only touched the surface, since medical device authorities can collaborate with both those that cover data protection, administrative law, criminal law, critical infrastructure and more to fulfil their positive obligations.

ment in the hospital system, medical device security touches many aspects of public law at once, even if it is initially "just" product regulation.

The chapter has in this way answered the purpose of analysing the interaction between law and security, and done in the manner above.

Below is a summary of the findings, which are included for the sake of clarity.

3.9.1 Findings

It was shown that the MDR that governs surgical robots does not on its face consider security aspects. There are considerations about the health and safety of patients, but not specifically about the risk that adversarial attacks pose, nor are surgical robots explicitly mentioned.[207] Only the guidance that comes with the regulation, as well as an expanded interpretation on its rules of the risk and quality management systems come close to outright requiring a focus on security.

The other weakness which the MDR has, which is regulatory capture, can be dealt with via the framework of intention. As the MDR allows for direct intention, but in a manner where the manufacturer has a choice whether their product is a medical device or not, this also allows for potentially rampant circumvention. Direct and indirect intention solves this and is within the remit of the authorities to decide and use. The downside of this approach is increased burdens on the entire system, but it would require currently unregulated software and hardware to have better security, which in turn could make the patient safer. The latter is especially prudent due to the potential mental health effects which supposed diagnosis or health apps can have, even though most of them have not been certified as medical devices.

[207] However, this is very understandable due to the technology neutral nature of the Regulation.

As for other EU legislation, there is a possibility that the EU can take subsidiary measures to address out what the regulation misses.[208] This can be interpreted as several obligations for manufacturers, including security, and since they explicitly require elimination of risks and security levels, and proper functioning of the medical devices,[209] they have a higher chance of working in a cumulative manner, and ensure security despite its more general wording. It furthermore burdens the manufacturer (because of the increased obligations), which if breached when it comes to security and defences in the surgical robot, can be used effectively to support careless behaviour in civil litigation.

Furthermore, there is the possibility of future legislation down the line, as well as the current rights of regulators to inspect, withdraw and generally keep a close eye upon the surgical robots if they are willing to do so.[210] The authorities' use of rights has yet to be seen regarding adversarial attacks on surgical robots, and while useful, there is no guarantee that the regulators have the staff or finances for it.

Regarding the application of Danish Law to the situation of a surgical robot suffering an adversarial attack, the chapter finds that the issue of proving anything in court can be a major obstacle for lawsuits. Design documentation, log files and other documentation that the manufacturer has access to is not initially able to the patient. But because civil lawsuits rely on free argumentation from both parties, the patient can indirectly force such proof out, or via the MDR.[211]

The chapter finds a lawsuit based on product liability possible, if it is based on the EU directive or case law based approach in Danish law,[212] but not if

[208] See preamble 101 of the MDR.

[209] Which means that adversarial attacks must be mitigated so as to make the devices work as intended at all times.

[210] See e.g., Art 10(14) in the MDR.

[211] See Art 10(14).

[212] To use the case law approach for litigation, the Product Liability Directive must not

it is based on contract.[213] The two useful types of lawsuit require that the surgical robot be put into circulation, so completely custom made versions are exempted. Especially the use of *res ipse loquitur*, which is showing that nothing else, but an adversarial failure could have caused it, is likely a very efficient approach in court. This, supported by case law, shows the link between the defect and the injury, but the defendant has one last defence they can ask for which the case law is based test of "systemic damage". If the danger adversarial attacks pose is known and unavoidable, the defect can be disproved, and the patient will most likely lose. But both questions have to be answered negatively in most situations, because the risk of attacks are not known by the public for the product, and only subversion of robotic control as an attack can be considered unavoidable.

The chapter shows that the patient is able to sue for damages via reimbursement outside of contract, but proving the link between the attack and the injury is difficult. Indeed, if the attack was subversion of robotic control, which involves factors outside of the surgical robot itself, the link is likely impossible to prove. And the patient can further attempt to argue that the needed knowledge is kept so closely to the other party, that it would be better shown if the judge reverses the burden of proof, which would bypass all needs to prove any criteria necessary to use this approach and instead force the manufacturer to prove that the surgical robot is designed appropriately, which is a direct reversal of the burden of proof.

And finally, the most secure way to cover damages, is to make use of the Patient Compensation system. Instead of suing the manufacturer of the robot that was attacked, the patient can choose to submit a free application to the Danish Patient Compensation Association, and get their damages

be applicable.

[213]This approach requires there to be a contract between the patient and the manufacturer of the surgical robot, which there is not, but future case law could reveal a new way to interpret this approach.

fully covered.[214] This is only between the state and the patient, which means it is cheaper and easier for the manufacturer of a surgical robot. It is sure to succeed because the rules surrounding this dictate, that if the machine fails, no matter the cause, the patient is entitled to have all their damages fairly covered.

[214]If they were deemed to have been injured.

4 | Client-side Scanning and Human Rights Law; an uneven match?

4.1 Introduction

Mass surveillance is not a new phenomena,[1] and a contemporary way to commit and complete the task now exists through digital mass surveillance.[2] With the advent of a digital society,[3] surveillance is conducted on almost all hardware and software, and this increased during the COVID-19 crisis via digital health surveillance.[4] As with any type of digital technology, there is also a security angle that is worth considering,[5] which this chapter focuses on. Surveillance may face obstacles in the form of Human Rights Law, something which this chapter analyses too as an example of boundaries and limits.

[1] Yekutieli (n 15); David Lyon, *State and Surveillance* (techspace rep, Centre for International Governance Innovation 2019).

[2] Stoycheff, Burgess, and Martucci (n 15).

[3] Jørgensen (n 8).

[4] Sharifah Sekalala and others, "Analyzing the human rights impact of increased digital public health surveillance during the COVID-19 crisis" (2020) 22(2) Health and Human Rights 7; Taylor and others (n 4); David Lyon, *Pandemic Surveillance* (John Wiley & Sons 2021).

[5] Harold Abelson and others, "Keys under doormats: Mandating insecurity by requiring government access to all data and communications" (2015) 1(1) Journal of Cybersecurity 69; Peter Fussey and Ajay Sandhu, "Surveillance arbitration in the era of digital policing" (2022) 26(1) Theoretical Criminology 3.

To make it more specific, an example of surveillance technologies is taken in the form of *Client-side scanning (CSS)*.[6] The cybersecurity community broadly distinguishes between two types of scanning: server-side[7] and CSS. CSS used on individuals for surveillance has been criticized,[8] which contrasts support for its usage in some contexts.[9] Most current surveillance is done via server-side scanning, while existing software such as antivirus programs use CSS.[10] Furthermore, CSS analyses the content before it is encrypted, unlike server-side, which may create additional cybersecurity risks and potential failures. CSS therefore adds a whole new level of surveillance, as these systems may track everything, on a specific system or device, in real-time.[11]

Currently, few taxonomies and comprehensive theoretical systems on CSS exist.[12] This chapter will contribute with one in the form of *a definition*, to increase the understanding of how CSS will impact security, which in turn answers how it could be regulated by the law. The chapter also brings an abstract overview of the possible type of attacks on generic CSS and

[6]Client-side refers to *on something*, which could be on a web client, or the device itself, such as a smartphone or a computer.

[7]Servers are a computer, or similar, which is not the one you are committing an action on, and which may store or provide a service to you on your own device. See also Florian Hantke and others, "Where Are the Red Lines? Towards Ethical Server-Side Scans in Security and Privacy Research" (2024).

[8]Hal Abelson and others, "Bugs in our Pockets: The Risks of Client-Side Scanning" (_eprint: 2110.07450, 2021) ⟨http://arxiv.org/abs/2110.07450⟩.

[9]Lisa Geierhaas and others, "Attitudes towards Client-Side Scanning for CSAM, Terrorism, Drug Trafficking, Drug Use and Tax Evasion in Germany" (IEEE May 2023) ⟨https://ieeexplore.ieee.org/document/10179417/⟩ accessed 28 September 2023.

[10]See Ori Or-Meir and others, "Dynamic Malware Analysis in the Modern Era—A State of the Art Survey" (2020) 52(5) ACM Computing Surveys 1 ⟨https://dl.acm.org/doi/10.1145/3329786⟩; Fred Cohen, "Computer Viruses - Theory and Experiment" (1987) 6.1 Computers & Security 22 ⟨all.net/books/virus/⟩.

[11]An analogy to this, could be the illustration of going from an agent occasionally tracking you and watching your house, to the agent living in your house and occasionally searching through your belongings.

[12]Shubham Jain, Ana-Maria Cretu, and Yves-Alexandre de Montjoye, "Adversarial Detection Avoidance Attacks: Evaluating the robustness of perceptual hashing-based client-side scanning" [2022] USENIX Security 2022; Guanxiong Ha and others, "Threat Model and Defense Scheme for Side-Channel Attacks in Client-Side Deduplication" (2023) 28(1) Tsinghua Science and Technology 1 ⟨https://ieeexplore.ieee.org/document/9837022/⟩ accessed 23 September 2023.

comments about adversaries through a threat model.

CSS, as surveillance often does, may affect Human Rights; thus, the other primary focus of this chapter is analysis of whether CSS will violate Human Rights Law, or how CSS can be used legally in the same context, through the European Convention on Human Rights (ECHR). This chapter does not suggest that human rights apply directly to manufacturers of CSS; the primary focus is on how Human Rights Law applies to states in the form of obligations, and the negative effects of CSS through this lens. The ECHR is notorious for its case law, which is continuously updated and held against the age which it is created in.[13] This is both a strength and a weakness of the system, as it is often accused of being reactionary. The problem painted here also constitutes the framework in which two central questions of thesis will be answered.[14]

The chapter initially uses an example of CSS, Apple's Child Sexual Abuse Material detection system (CSAMD). This system has been postponed indefinitely, but this does not make the discussion of it and future similar systems any less important, as it would have applied to all iPhones and the iCloud. Apple is likely not the only company to have such a system, but they are, as of the time of writing, the only company to have publicly released proofs and system summaries,[15] and publicly answered why they retracted their system.[16] CSAMD was created to fight CSAM (Child Sexual Abuse Material), which is considered a crime in a majority of the jurisdictions of the world.[17] Preventing such material to be uploaded and

[13]Françoise Tulkens, "Judicial Activism v Judicial Restraint: Practical Experience of This (False) Dilemma at the European Court of Human Rights" (2022) 3(3) European Convention on Human Rights Law Review 293 ⟨https://brill.com/view/journals/eclr/3/3/article-p293_002.xml⟩ accessed 28 September 2023.

[14]"How can this legal concept be understood in cybersecurity," and "how can these cybersecurity considerations be understood in law"?

[15]Abhishek Bhowmick and others, *The Apple PSI System* (techspace rep, 2021).

[16]See https://appleinsider.com/articles/23/08/31/apple-provides-detailed-reasoning-behind-abandoning-iphone-csam-detection, last accessed 11 December 2024.

[17]Abhilash Nair, "Internet Content Regulation: Is a Global Community Standard a

spread is vital, but this is usually left to authorities of individual national states, or cooperation via NGOs. Outside of Criminal Law, mental health surveillance is also done through apps[18] or through traditional means of data gathering.[19] CSS transcends these features as surveillance, since, in the case of the CSAMD, it is done on the system at large.

This chapter provides a very short commentary on the potential usage and consequences in the fight against CSAM with two pieces of legislation; the UK's Online Safety Act,[20] and EU's proposed Child Sexual Abuse Regulation.[21] Both of these suggest using CSS on all messaging platforms, making them relevant to include specifically in this chapter, as the observations made about CSS and the ECHR apply directly to these two pieces of legislation. This is both due to their technology specificity, and due to their status as statutory legislation, subservient to the *lex surperior* status of the ECHR in both UK and EU Law.[22]

The chapter is therefore structured as follows: Section 2 introduces the taxonomy for a general understanding of attacks and adversaries for CSS, and discusses it at a general level, section 3 discusses the case of the CSAMD, section 4 analyses human rights, specifically Article 6, 8, 10 and 11 of the ECHR in the context of CSS. Section 5 discusses the Online Safety Act and the Child Sexual Abuse Regulation, section 6 includes future consid-

---

Fallacy or the Only Way Out?" (2007) 21(1) International Review of Law, Computers & Technology 15.

[18]Lisa Cosgrove and others, "Digital phenotyping and digital psychotropic drugs: Mental health surveillance tools that threaten human rights" (2020) 22(2) Health and Human Rights 33.

[19]Rebecca A Johnson and Tanina Rostain, "Tool for surveillance or spotlight on inequality? Big data and the law" (2020) 16 Annual Review of Law and Social Science 453.

[20]https://bills.parliament.uk/bills/3137, last accessed 11 December 2024.

[21]European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (2022) ⟨https://ec.europa.eu/home-affairs/system/files/2022-05/Proposal%20for%20a%20Regulation%20laying%20down%20rules%20to%20prevent%20and%20combat%20child%20sexual%20abuse%7B%5C_%7Den%7B%5C_%7D0.pdf⟩.

[22]In EU Law, it is done through the Charter of Fundamental Rights of the European Union.

erations and section 7 is the conclusion.

In the following section, the security aspects of CSS are explored, which lay the foundation for the rest of the chapter.

4.2 Cybersecurity Considerations

Some general comments on the threat modelling and adversaries which CSS brings will be addressed in this section. These are based on existing taxonomies and literature on CSS and security in general and attempt to combine and improve these to provide a more compact, abstract, and comprehensive overview for both security and legal practitioners.

4.2.1 CSS Definition

CSS is on-device analysis of data,[23] which is different from analysis from information gathered elsewhere. The general distinction is between server-side[24] and client-side, though hybrids and combinations between the two exist. The last S in CSS, scanning, is central for when CSS occurs, as just keeping an eye on some parts of a client-side system is not CSS. It must cover the whole category which it focuses on. This leads us to a definition that could be as follows:

Client-side Scanning is the action of on-device scanning of contents, be it pictures, text, audio, telemetry, or otherwise, in real-time or at a later point. Later point is included, because *ex post* analysis with transparent or clear logs can reveal what happened for analysis at a later date, though this could be a venue for defences against CSS too.

[23] Abelson and others (n 8).

[24] Cloud Service server-side scanning of the content which uploaded, to detect violations of their terms of service, is a good example of server-side scanning.

Other authors focus on CSS purely being a review mechanism,[25] which clashes with how antivirus and similar software has always functioned, or have narrowly focused on for example Apple's definition of CSS in their proposal for a system.[26] Both of these can work in context, but do not cover CSS generally.

Our broader definition covers firewalls, antivirus,[27] and any type of surveillance system on smartphones, computers, or any digital device, which passively scan contents on client-side.[28]

4.2.2 Threat Model and Adversaries

Due to the influence and significance of client-side web threats, several taxonomies and threat models are built after these.[29] This is not a disadvantage, as there is a certain overlap both in the understanding and practical reality between websites and software from a client perspective. Clients are susceptible to a range of attacks which naturally appear from browsing, from the infrastructure or on the website, or the internet in general.[30] This is mirrored in the software side of CSS. Another angle which is covered in the literature, is trust, as understanding and quantifying the trust which the client must have, versus the risk and reality of client-side attacks is also

[25] Paul Rosenzweig, "The Law and Policy of Client-Side Scanning" (2020) 58 Joint PIJIP/TLS Research Paper Series, 4.

[26] Geierhaas and others (n 9).

[27] Jolynn Childers Dellinger and David Hoffman, "You Are Being Scanned" (2022) 106(3) Judicature, 74.

[28] CSS can also be misused in a variety of ways, see Shubham Jain and others, "Deep perceptual hashing algorithms with hidden dual purpose: when client-side scanning does facial recognition" (IEEE May 2023) ⟨https://ieeexplore.ieee.org/document/10179310/⟩ accessed 29 April 2024.

[29] Daniel Hein, Serhiy Morozov, and Hossein Saiedian, "A survey of client-side Web threats and counter-threat measures: Client-side Web threats and counter-threat measures" (2012) 5(5) Security and Communication Networks 535 ⟨https://onlinelibrary.wiley.com/doi/10.1002/sec.349⟩ accessed 23 September 2023; Yassine Sadqi and Yassine Maleh, "A systematic review and taxonomy of web applications threats" (2022) 31(1) Information Security Journal: A Global Perspective 1 ⟨https://www.tandfonline.com/doi/full/10.1080/19393555.2020.1853855⟩ accessed 23 September 2023.

[30] Sadqi and Maleh (n 29) 17.

important.[31] This kind of trust, which relies on intent and behaviour, tends to be weak against intentionally malicious code,[32] which explains why it is not further analysed in this chapter.

Initially, CSS, whether in antivirus software or otherwise, add an additional angle to the security of any given system. For antivirus, the measure must outweigh the costs. The problem with CSS when applied outside of antivirus, is that the actions only serve the manufacturer, not the user or the subjects of the system.[33]

Antivirus and other similar programs provide security in exchange for CSS and other data gathering activities, while both risking security and privacy failures. Security, as the CSS could be hijacked or otherwise manipulated by adversaries, and privacy, because the personal data gathered can be misused if stolen by an adversary later. Both things can happen to non-CSS software too, but this kind of scanning action leaves the systems vulnerable from their inception. Other software which is compromised may not have access to the same kinds of tools which those that deploy or are CSS do.

On the other hand, non-antivirus CSS provides no advantages for users or subjects. Their CSS measures exist for legal compliance, or semi-compliance, or actions which are masked as compliance, including premises such as "safety".[34] This makes the system decidedly unequal, and comparisons to poor personal data gathering can be made, though CSS has far graver consequences than personal data gathering being hijacked by adversaries.

[31] Hein, Morozov, and Saiedian (n 29) 6 - 7.

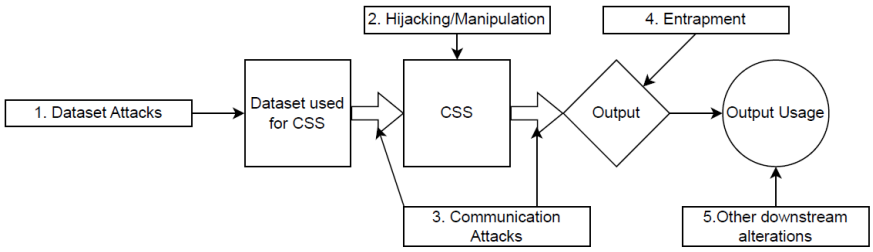
[32] Victor Prokhorenko, Kim-Kwang Raymond Choo, and Helen Ashman, "Web application protection techniques: A taxonomy" (2016) 60 Journal of Network and Computer Applications 95 ⟨https://linkinghub.elsevier.com/retrieve/pii/S1084804515002908⟩ accessed 23 September 2023, 16.

[33] Abelson and others (n 8).

[34] There is often no public safety analysis done to justify this last marker. This goes against existing safety engineering methodology, Leveson (n 163); Nancy Leveson and John P Thomas, *STPA Handbook* (2018); Nancy G Leveson, CAST Handbook: How to Learn More from Incidents and Accidents (2019).

With the inequality being established, we can move on to a CSS threat model, which includes an overview of the possible attacks. It is deliberately abstract, and does not numerically encompass every single attack, but instead has overarching categories which are fitted to the notion of CSS as such. This is input, datasets, which feeds into and shapes the CSS, output from the CSS, and output usage.

Figure 4.1: Illustration of possible attacks which CSS generically can incur.



1. Dataset Attacks.

2. Hijacking or Manipulation Attacks.

3. Communication Attacks.

4. Entrapment.

5. Other downstream alterations.

All these attacks can be connected, one may cause the other, or enable several of the others to occur later.

Dataset Attacks This refers to a range of attacks where an adversary attacks the datasets or information which the CSS system builds its models on. This can both be used in ML (machine-learning)[35] and non-ML systems, as there will be information used to create either type. For systems that will resemble that which Apple proposed in 2021, the data needed is stored on the device, meaning that there is a risk that the adversary can manipulate this information purely on one device, and not necessarily on

[35]Florian Jaton, "Assessing biases, relaxing moralism: On ground-truthing practices in machine learning design and application" (2021) 8(1) Big Data and Society.

a system-wide scale. The range of attacks covered are poisoning, replacement, or deletion, but all refer to manipulation of the data to cause changes downstream in the CSS system.

Hijacking or Manipulation Attacks This only concerns direct manipulation or hijacking (control) of the CSS. These are in the same category because they create the same outcome, which is direct changes in the CSS, in real-time or otherwise. These can lead to adverse outcomes or halt the CSS entirely. The latter is important if the CSS is necessary to authenticate or otherwise enable different processes outside the system. Recently, CSS has been used to include physical surveillance[36] which was and is not intended by any current manufacturers of CSS.

Communication Attacks These target the communication between the CSS, or the communication between analysis or the dataset which the CSS makes use of.[37] This can change the output, and lead to the fourth attack below, or otherwise scramble or distort the CSS output, which may disable it. It can also distort the data which the CSS model uses, which can cause similar outcomes far earlier.

Entrapment This is similar to the second attack, but instead of controlling or changing the CSS as such, the output is changed. This has already been proven possible experimentally.[38] It is called entrapment because that is its primary purpose, but it could also include deletion or similar. The issue with the latter is the outcome, which from the perspective of law en-

[36] Ashish Hooda and others, Re-purposing Perceptual Hashing based Client Side Scanning for Physical Surveillance (arXiv:2212.04107 [cs], arXiv December 2022) ⟨http://arxiv.org/abs/2212.04107⟩ accessed 28 September 2023.

[37] Coverage of communication from the output and onward is covered in the fifth attack below.

[38] Jonathan Prokos and others, "Squint Hard Enough: Attacking Perceptual Hashing with Adversarial Machine Learning" (2023); Re-purposing Perceptual Hashing based Client Side Scanning for Physical Surveillance (n 36).

forcement may be the same, as any kind of unknown changes could lead to suspicion and potential investigation. Entrapment is discussed later in this chapter, but is a widely used tool by law enforcement, and can be used directly by other adversaries as well, regardless of the type of CSS.

Other downstream alterations This is a broad category which covers additional changes or manipulation with the processes which use the output. These attacks are therefore not what can be seen in the fourth attack, but instead target subsystems, and have more of a generic nature. The reason for their inclusion is their connection to the output and being part of the broader CSS system. In this sense, the type of failures they can cause are like earlier attacks but have a distinctly different origin.

Adversarial actors can be limited to the following: Manufacturers, foreign governments, cybercriminals, terrorists.[39] Manufacturers themselves may also be powerful societal actors, which can be seen in the case in the next section for companies such as Apple, with an economic presence the same size as a small national state. These can have interest in maliciously complying with or circumventing compliance with the CSS system they themselves create and run, and there is nothing preventing them from working with any of the other adversarial actors. Foreign governments have a large amount of manpower, enabling sophisticated attacks against CSS, to target individuals, groups, or dissidents. Cybercriminals, like elsewhere, may target CSS for profit, also against the manufacturer, but may also attack on orders from other adversaries. Terrorists would target CSS to disrupt society, or to cause some kind of wide-spread damage; both depend on the CSS in question.

In the next section, an example of CSS is considered.

[39]There are arguments to make for including "individuals" as its own group, but these are included under the envelope of cybercriminals.

4.2.3 CSAMD

Apple documents its proposed Child Sexual Abuse Material Detection system in a variety of online documents.[40]

A less overarching but more detailed analysis of the system has been done elsewhere,[41] its NeuralHash image tool[42] has been reverse engineered several times,[43] and another image tool akin to it has also been reverse engineered and found vulnerable.[44]

The proposed detection system is based on a range of techniques: private set intersection (PSI),[45] Cuckoo tables,[46] Secret sharing, Diffie-Helman problems[47] and hardness, Naor-Reingold Diffie-Hellman[48] random self-reducibility, Coppersmith and Sudan Algorithms,[49] Interleaved Reed-Solomon

[40] Apple Inc, "CSAM Detection - Technical Summary" (Issue: August, 2021) ⟨https://www.apple.com/child-safety/pdf/CSAM%7B%5C_%7DDetection%7B%5C_%7DTechnical%7B%5C_%7DSummary.pdf⟩; Bhowmick and others (n 15); Mihir Bellare, *A Concrete-Security Analysis of the Apple PSI Protocol* (techspace rep, Apple 2021) ⟨https://www.apple.com/child-safety/pdf/Alternative%7B%5C_%7DSecurity%7B%5C_%7DProof%7B%5C_%7Dof%7B%5C_%7DApple%7B%5C_%7DPSI%7B%5C_%7DSystem%7B%5C_%7DMihir%7B%5C_%7DBellare.pdf⟩.

[41] Benny Pinkas, The Private Set Intersection (PSI) Protocol of the Apple CSAM Detection System (Publication Title: Decentralized Thoughts, 2021) ⟨https://decentralizedthoughts.github.io/2021-08-29-the-private-set-intersection-psi-protocol-of-the-apple-csam-detection-system/⟩.

[42] For another perspective which is not much more positive, see Gabriel J Rudin, "Walling off Privacy: Apple's NeuralHash Controversy, the ECPA, the Fourth Amendment, and Encryption" (2023) 21(2) Colorado Technology Law Journal.

[43] Lukas Struppek and others, "Learning to Break Deep Perceptual Hashing: The Use Case NeuralHash" (_eprint: 2111.06628, 2021) ⟨https://arxiv.org/abs/2111.06628v1⟩.

[44] Anish Athalye, Inverting PhotoDNA (2021) ⟨https://www.anishathalye.com/2021/12/20/inverting-photodna/⟩.

[45] Peter Rinda and Mike Rosulek, "Malicious-Secure private set intersection via dual execution" [2017] Proceedings of the ACM Conference on Computer and Communications Security 1229 (ISBN: 9781450349468).

[46] Rasmus Pagh and Flemming Friche Rodler, "Cuckoo Hashing" in *BRICS Report Series* (ISSN: 0909-0878, August, 2001) ⟨http://link.springer.com/10.1007/3-540-44676-1%7B%5C_%7D10⟩.

[47] Jiaxin Pan, Chen Qian, and Magnus Ringerud, "Signed Diffie-Hellman Key Exchange with Tight Security" in *Topics in Cryptology – CT-RSA 2021* (2021).

[48] Thierry Mefenza and others, "Polynomial interpolation of the generalized Diffie–Hellman and Naor–Reingold functions" (2019) 87 Designs, Codes and Cryptography 75 (ISBN: 1062301804861).

[49] Don Coppersmith and Madhu Sudan, "Reconstructing curves in three (and higher) dimensional space from noisy data" [2003] Conference Proceedings of the Annual ACM Symposium on Theory of Computing 136 (ISBN: 1581136749).

code under random noise and tuples.[50] The idea of private set intersection refers to primary set theory properties like $A \cup B$ (intersection). The main notion being that CSAMD is a complex system, which rightfully fuses several privacy and security enhancing technologies at once.

The CSAMD uses secret sharing to find this intersection, which is done between the user, Apple, and the system. Letting Apple control the system tool which one relies on for secret sharing is problematic, you do not want to share the real intersection, so $A' \cup B'$ is used instead.

The CSAMD uses Shamir Secret Sharing, which means that the secret is an element of a finite field ($s \in \mathbb{F}$), of which a polynomial with a certain degree is picked. Because of the qualities of the finite field, shares of the secret can be created which rely on the polynomial, and then there exists a threshold for which the polynomial can be guessed.

But if the system cannot get the necessary number of shares to reach the threshold, only the user and Apple will know the secret. In the CSAMD, this is further modified so that not even the system nor Apple will know through synthetic shares, which are periodically uploaded by the user.[51]

But will the system know when it is handling synthetic or real matches? As the data sent by the users is put into cuckoo tables to hash the data, cuckoo hashing uses two functions with a set size and two tables, where the key (in this case) can exist in both tables but never both at the same time.[52] Each function will be sent every time, regardless of whether the key is in one or the other. In this context, Diffie-Hellman hardness is used to assert how negligible the success of an adversarial attacker in guessing different elements of the tuple and a property of the tuples is, and Diffie-Hellman random self-reducibility is a means to use the fact that Diffie-Hellman tu-

[50] Daniel Bleichenbacher, Aggelos Kiayias, and Moti Yung, "Decoding of Interleaved Reed Solomon Codes over Noisy Data" (ISSN: 16113349, 2003) vol Lecture No.

[51] Apple Inc (n 40).

[52] Pagh and Rodler (n 46).

ples are not random tuples.[53] The latter is a core part of the creation of the key mentioned above. The shares (central to PSI) which are correct among the synthetic ones can be detected with the interleaved Reed-Solomon under random noise algorithm,[54] which relies on the relationship between the values, and these are kept under control by always including a version of the picture in lower resolution, limiting the size to one which the algorithm satisfies its parameters.

Safety Comments and Criticism

There has been public criticism by prominent authors,[55] explicitly of NeuralHash[56] and similar future schemes.[57]

What can be agreed upon, is that CSAMD may fail to detect CSAM, because it is not within its known data set, or the adversary abuses NeuralHashing, or by other measures. This can be done both to abuse the system (to i.e. target individuals) or to hide CSAM as such.[58] There therefore exists a risk of the ML model being abused or circumvented.

Struppek et al.[59] present arguments which show that NeuralHash is not fit for purpose. 90 to 100 percent success rate[60] of an adversarial attack, show that NeuralHash is not robust against simple image processing software. This may indicate problems with deep perceptual hashing employed in this manner in general, and not just on images. *Struppek et al.* also showed

[53]The Private Set Intersection (PSI) Protocol of the Apple CSAM Detection System (n 41).

[54]Bleichenbacher, Kiayias, and Yung (n 50); The Private Set Intersection (PSI) Protocol of the Apple CSAM Detection System (n 41).

[55]Jonathan Mayer and Anunay Kulshrestha, Opinion: We built a system like Apple's to flag child sexual abuse material — and concluded the tech was dangerous (Publication Title: The Washington Post, 2021) ⟨https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/⟩.

[56]Struppek and others (n 43).

[57]Abelson and others (n 8).

[58]Struppek and others (n 43).

[59]ibid.

[60]ibid.

that NeuralHash leaks from its classifiers, which is not unexpected, but further justifies not using any technique like NeuralHash when handling potentially sensitive or private information, as this may lead adversaries to be able to infer information or perhaps more without having access to the entire image. The use of Neural Networks will always enable the risk of the attacks mentioned by the authors, which means they should not be used until suitable defences are found.

An increased risk of security and privacy violations may occur if the materials are later de-encrypted and then judged by a human in-the-loop in the CSS system, who is not part of law enforcement of any state. By itself, having this additional link on the chain between CSS and states provide a greater attack surface. Safeguards which NGOs[61] and other structures that may include specialists can give are not necessarily enough, as they will still not be faced with ethical and legal rules of conduct or enjoy the legitimacy of being hired by a state, which civil servants of states are. This does not prevent efficient and useful relationships between such NGOs like those who would have played a role in the CSAMD and states, but it presents an additional privacy and security threat.

Moving on to the potential Human Rights Law aspects of CSS, some of these lacking legal guarantees are further discussed in the next sections.

4.3 Human Rights Law Considerations

As indicated earlier, CSS systems may cause Human Rights Law violations.[62] The potential which CSS inspired by the CSAMD may have in the

[61] Ben Wagner, "The Politics of Internet Filtering: The United Kingdom and Germany in a Comparative Perspective" (2014) 34(1) Politics 58.

[62] Privacy violations seem clear from its inception, because it is inherently constant on-device surveillance, and contextual privacy and clearer consent rules will not solve these problems, Mohamad Gharib, "Privacy and Informational Self-determination Through Informed Consent: The Way Forward" (2022) 13106 LNCS Lecture Notes in Computer

future too present concrete ideas for violation of Human Rights, as will be discussed below. On the other hand, CSS and data protection rules interact in a different manner,[63] and represents a more hands-on approaches in the form of Data Protection Impact Assessments.[64] Data Protection perspectives are not the focus of this chapter, other authors have handled the matter elsewhere.[65] Data Protection rules are, however, not equivalent to applying Human Rights Law, though the connection exists,[66] and may in the future become stronger.[67]

The ECHR as an instrument was created by the Council of Europe, which includes EU Member States, and additional countries. The EU has the Charter of Fundamental Rights of the European Union, which uses and expands the ECHR. The ECHR exists above national legal systems, which is necessary for it to function.[68] For a citizen in these countries, the European Court of Human Rights (ECtHR)[69] is the last resort.[70] Before going to the ECtHR, it is up to the national judges, civil or otherwise, to apply

Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 171 (ISBN: 9783030954833).

[63]Jennifer Cobbe, "Data protection , ePrivacy , and the prospects for Apple's on-device CSAM Detection system in Europe" (2021) ⟨https://osf.io/preprints/socarxiv/rhw8c/⟩.

[64]Reuben Binns, "Data protection impact assessments: a meta-regulatory approach" (2017) 7(1) International Data Privacy Law 22 ⟨https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipw027⟩ accessed 26 February 2024.

[65]Cobbe, "Data protection , ePrivacy , and the prospects for Apple's on-device CSAM Detection system in Europe" (n 63); Rosenzweig (n 25).

[66]

Alessandro Mantelero and Maria Samantha Esposito, "An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems" (2021) 41 Computer Law & Security Review 105561 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364921000340⟩ accessed 26 February 2024.

[67]Alessandro Mantelero, "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment" (2018) 34(4) Computer Law & Security Review 754 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364918302012⟩ accessed 26 February 2024.

[68]Besson (n 148).

[69]Long criticised for their style of ruling, but on the contrary, see George Baboulene, "Has the elastic interpretation of human rights law led to the 'living instrument' approach to the ECHR interpretation being inherently flawed?" (2023) 48 Exeter Law Review.

[70]In this section, cases are written normally, but the relevant paragraph is denoted with § instead of para, due to the different legal source and style. Also note that the case law used in this section, while valid, has been updated in the freely available guides from the ECtHR, meaning that current case law may differ. For updated guides, see https://ks.echr.coe.int/en/web/echr-ks/, last accessed 11 December 2024.

the ECHR properly. It is within this substance that judges and the systems as such must make these rights into reality.[71]

The following sections are a direct analysis as to *when* CSS systems can or cannot breach the ECHR based on several articles. This is in the form of tests or requirements from case law.

4.3.1 Right to a Fair Trial

CSS could impact the Right to a Fair Trial (Article 6), if evidence gathered by CSS is used in court or during investigation. While this chapter does not discuss the *Encrochat* case, *Stoykova* has analysed this in regards to fair trial.[72] The parallels to CSS are clear, but since *Encrochat's* main feature was encrypted communication, and its client-side scanning abilities only occurred when the service was hijacked by relevant authorities, it does not quality for the discussion of this chapter, outside of the part discussing entrapment.

Article 6 can apply if the individual is "charged with a criminal offense" or concerning civil cases through "civil rights and obligations". The criminal aspect is the focus of this chapter, but a civil litigation analysis of the role of CSS should be further investigated elsewhere. Charged does not only refer to when criminal proceedings have begun, but also before or when the suspicion is purely within the authorities and has not led to any initial procedural steps.[73] The rest of this section does not analyse Article 6 in an overarching manner but focuses on a specific aspect.[74]

[71] With the criticism that walking such a fine line brings, see e.g., Tulkens (n 13).

[72] Radina Stoykova, "Encrochat: The hacker with a warrant and fair trials?" (2023) 46 Forensic Science International: Digital Investigation 301602 ⟨https://linkinghub.elsevier.com/retrieve/pii/S2666281723001142⟩ accessed 26 July 2023.

[73] 31816/08, Stirmanov v. Russia, § 39.

[74] For more on how Article 6 has issues with AI, which are tangential to this discussion, see Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI" (2021) 41

The Right to Remain Silent and Not Incriminate Oneself

The Right to Remain Silent and Not Incriminate Oneself is not mentioned explicitly in Article 6 but is accepted through case law.[75]

The right implies that suspects have the option not to speak and not give information which would incriminate them.[76] The negative limit is to prevent evidence obtained through coercion or oppression[77] from being used. The exception is where the evidence is obtained through compulsory powers, such as lawful authorisation, of which the evidence must have an independent existence of the subject. This is in case law defined as blood,[78] which can be extrapolated as other bodily fluids, but not static things like pictures or physical objects. In practice, this means that they are *not* protected by the Right to Remain Silent and Not Incriminate Oneself, and can be used to initiate proceedings if matching evidence at a crime scene or similar.

Contrarily, CSAMD makes use of pictures which *do not have an independent existence of the subject*, and other CSS which analyse text or other variables should not be defined as such either.[79]

Computer Law & Security Review 105567 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364921000406⟩ accessed 28 September 2023.

[75] 10828/84, Funke v. France, § 44. For analysis of the right, see Tuomas Hupli, "To Remain or Not to Remain Silent: The Evolution of The Privilege against Self-incrimination Ten Years After Marttinen v. Finland" (2018) 6(2) Bergen Journal of Criminal Law and Criminal Justice 136; Javier Escobar Veas, "A Comparative Analysis of the Case Law of the European Court of Human Rights on the Right against Self-Incrimination" (2022) 8(2) Revista Brasileira de Direito Processual Penal ⟨https://revista.ibraspp.com.br/RBDPP/article/view/675⟩ accessed 28 September 2023; Mark Berger, "Self-Incrimination and the European Court of Human Rights: Procedural Issues in the Enforcement of the Right to Silence" (2007) 514 European Human Law Review; Andrew Ashworth, "Self-Incrimination in European Human Rights Law - A Pregnant Pragmatism" (2008) 30(3) Cardozo Law Review; Mark Berger, "Europeanizing Self-Incrimination: The Right to Remain Silent in the European Court of Human Rights" (2006) 12(2) Columbia Journal of European Law.

[76] This applies outside of criminal law too, Hupli (n 75).

[77] 19187/91, Saunders v. the United Kingdom, § 68 - 69

[78] 19187/91, Saunders v. the United Kingdom, § 68 - 69.

[79] Many jurisdictions may violate self-incrimination through current practice, like the analysis of social media posts of potential refugees in the application process, Koen Leurs, "Communication rights from the margins: politicising young refugees' smart-

Lawful authorisation of CSS information could allow authorities to fulfil the criteria to not violate the Right to Remain Silent and Not Incriminate Oneself, and use the information gathered by the CSS.

If lawful authorisations do not systematically give access to CSS systems, a test must be done by national courts to consider whether the individual retains the right, which could deny authorities usage of the data:

- *The nature and the degree of the compulsion, the existence of relevant safeguards in the procedure, and the use of the obtained material.*

Compulsion is irrelevant, as the data is gathered covertly or in full knowledge of the user. The jurisdiction where this test takes place must have specialised legal and practical safeguards. Legal and practical safeguards refer to CSS being used fairly, which is an explicit public versus individual interest evaluation, but it cannot be the argument for why the Right to Remain Silent and Not Incriminate Oneself must be extinguished,[80] which has been established by the ECtHR.[81]

In summary, the use of CSS in criminal trials under the ECHR regime requires lawful authorisation, that the evidence must have an independent existence of the subject (e.g., not be blood), and if these are not fulfilled, the state must pass the ECtHR case law established test regarding compulsion, safeguards, and usage of the material.

Following this, we include further details within Article 6.

---

phone pocket archives" (2017) 79(6-7) International Communication Gazette 674. Pictures which are synonymous with private property would also fit this category, denying its independent existence of the subject.

[80] 54810/00, Jalloh v. Germany, § 97. This means the system itself should not be built to violate the right. Public interest cannot extinguish the very essence of the right.

[81] Like 34720/97, Case of Heaney and McGuiness v. Ireland, §§ 57 - 58.

Admissibility

The evidence must be admissible, which refers to whether evidence can be used at a trial or not.[82] Some states have rules against evidence obtained wrongfully or by other means of evaluation, which can lead to situations where the files or just the detection of them cannot be used in proceedings.[83] This creates two situations. Firstly, one where CSS evidence may not be usable, because it inherently creates data which could violate The Right to Remain Silent and Not Incriminate Oneself. Secondly, it may be used, but then by its very nature violate The Right to Remain Silent and Not Incriminate Oneself.

The Convention does not in detail analyse admissibility rules in each jurisdiction, as these must be done in national law and by the relevant courts,[84] but it evaluates whether the case was "fair" or not in the context of inadmissibility or admissibility. The fairness test is individual and must be done entirely on a trial to trial basis.[85] It seems unlikely that the ECtHR would decide on the opposite, situations where inadmissibility would lead to CSS data being unusable in court, due to the distance they take towards criticising or in-depth analysing national admissibility rules.

If the case is not deemed fair because of non-admissibility, some jurisdictions will close the current case, and others will continue but lead to

[82] See e.g., Ximei Wu and Abid Hussain Shah Jillani, "Admissibility of Lis Pendens in International Commercial Arbitration: A Comparative Insight of Different Legal Systems" (2020) 13(4) Journal of Politics and Law 134; Sowed Juma Mayanja, "Circumstantial Evidence and Its Admissibility in Criminal Proceedings: A Comparative Analysis of the Common Law and Islamic Law Systems" (2017) 67 Journal of Law, Policy and Globalization; G L Peiris, "The Admissibility of Evidence Obtained Illegally: A Comparative Analysis" (1981) 13(2) Ottawa Law Review.

[83] Erik Voeten, "The impartiality of international judges: Evidence from the European court of human rights" (2008) 102(4) American Political Science Review 417.

[84] 28490/95, Hulki Günes v. Turkey.

[85] These can become quite complicated, a good example of the situation where CSS detects something, law enforcement reacts, and the subject of the CSS may be forced or coerced to give up their rights can be seen in 51/1997/835/104, Guérin v. France [GC], § 43.

the accused being found not guilty. This may make CSS evidence usage different in the various parties to the ECHR.

Planted Evidence and Entrapment

Relating explicitly to the Right to a Fair Trial, a trial can never be fair if the accused cannot question the evidence,[86] which will be difficult if relying on CSS or black box systems. This is due to the nature of the scanning constantly on the device of the accused, and because of the hidden approach to the coding from a user perspective.

A trial cannot be fair either, if the evidence used was planted.[87] This can be done by an adversary who sends the accused a file containing something that triggers the scanning. Regarding CSAMD, steganography[88] is not likely to be able to pass NeuralHash,[89] but for future CSS systems this may not case. The court recognises the need for the investigative authorities to combat organised crime, but planting false evidence is not included in this. Finally, a trial cannot be fair if the evidence is obtained through unlawful secret surveillance,[90] which as a rule also will make such evidence inadmissible.

Entrapment is worth mentioning in the same vein.[91] This refers to various means to either frame or otherwise through "traps" to finds reasons to investigate individuals.[92] This could very well be done with CSAMD or

[86] See e.g., 36658/05, Murtazaliyeva v. Russia, § 91. The notion is effective participation in proceedings.

[87] 22062/07, Layijov v. Azerbaijan, § 64.

[88] Steganography is the science of hiding text, code, or otherwise, in something else, such as pictures.

[89] Nandhini Subramanian and others, "Image Steganography: A Review of the Recent Advances" (2021) 9 IEEE Access 23409 (ISBN: 0113180276).

[90] 35394/97, Khan v. the United Kingdom, § 34.

[91] In ECtHR case law, there is a distinction between planted evidence and entrapment, but as was indicated in Section 4.2.2 of this chapter, considering them together in a cybersecurity sense seems adequate regardless of their split else. For definition, see 74420/01, Ramanauskas v. Lithuania [GC], § 55.

[92] 59696/00, Khudobin v. Russia, § 128.

similar systems, with the exact same techniques as an adversarial attacker. Entrapment has happened in many states of the Council of Europe, including Croatia,[93] Germany,[94] Lithuania,[95] United Kingdom,[96] and more. Indirect entrapment, where other individuals or organisations are hired, is covered as well.[97]

However, entrapment can be allowed if the procedure passes the following two tests:

1. *The substantive test of incitement.* Police or other authorities must not have incited, directly[98] or indirectly,[99] the offense which the CSS then detects. This means analysing the behaviour of the authorities, and the institutions and rules surrounding the authorisation of the entrapment.[100]

2. *The procedural test of incitement.* This is a test of the courts. The national courts must carefully consider whether incitement took place,[101] allow the accused to defend and otherwise argue against the claims,[102] and the system in the courts must allow this in the legislation which regulates it.

If the CSS based entrapment passes both tests, it is allowed within the ECHR, and vice versa.

With this, we move towards a more privacy-centric analysis of the use of CSS.

[93] 47074/12, Grba v. Croatia.
[94] 40495/15, Akbay and Others v. Germany.
[95] 74420/01, Ramanauskas v. Lithuania.
[96] 67537/01, Shannon v. the United Kingdom
[97] 40495/15, Akbay and Others v. Germany, § 117).
[98] E.g., 17711/07, Sepil v. Turkey, 2013, § 34.
[99] Such as pretending to have committed the crime to indirectly incite the accused, see 74355/01, Milinienė v. Lithuania, §§ 37-38.
[100] See e.g., 66152/14, Kuzmina and Others v. Russia, 2021
[101] 74420/01, Ramanauskas v. Lithuania, §§ 70 - 72.
[102] 74420/01, Ramanauskas v. Lithuania, § 69.

4.3.2 Right to Respect for Private and Family Life, Home and Correspondence

Right to Respect for Private and Family Life, Home and Correspondence, Article 8, covers the protection of these terms in Article 8, part 1, but also protects from interference from public authorities in part 2. Exceptions to part 2 are *"in accordance with the law, is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

Article 8, part 1, explicitly has to do with the integrity and status of one's private pictures, including the protection of privacy.[103]

In the case law of the ECtHR, privacy is either protected positively or made to protect against the state negatively, but there exists a right for the individual to be protected against other private parties,[104] though this must still be facilitated by the State.[105]

Article 8 could potentially interfere with the use of CSS within national states. The Right to Privacy is not an absolute right,[106] but instead relies on the entirety of Article 8. Interfering in privacy requires a legitimate aim, and for the CSAMD, fighting CSAM would fit under "prevention of

[103] 40660/08 and 60641/08, Von Hannover v. Germany (no. 2), § 95. For an overview of how privacy cases are treated, see OL Van Daalen, "The right to encryption: Privacy as preventing unlawful access" (2023) 49 Computer Law & Security Review 105804 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364923000146⟩ accessed 28 September 2023, 2 - 5. Additionally, see Jakob Sjøberg, "European Convention of Human Rights and the Protection of Private Life, Freedom of Expression and Access to Information in a Digital Age" (PhD thesis, Arcada University of Applied Sciences 2023).

[104] 61496/08, Bărbulescu v. Romania [GC], §§ 112 - 112, to be understood in an expanded manner.

[105] This right for protection against private parties is a recognition of their new role in infringing privacy systematically. This allows Article 8 to be applied differently under certain circumstances, enabling individuals to sue the state over its lack of action against the private parties.

[106] Van Daalen (n 103) 14.

disorder or crime", "for the protection of health and morals", and "for the protection of the rights and freedoms of others"; therefore usually not an issue to prove in court.[107] This could be significantly different for other CSS systems, if their purpose is not related to criminal investigations.

The other test from part 2 of Article 8 however, is whether violating the right is "necessary in a democratic society". This is by the court interpreted directly into "pressing social need", which the interference must justify precisely, and it must be proportionate to the problem which needs to be solved.[108] A given state would then need to justify the surveillance through these rules, and for CSAMD (as announced by Apple), this has not been done adequately. There is no documentation that proves or makes it likely that there exists the huge amount of CSAM which would justify CSS on all devices, as the measure would only be proportionate if the pressing social need warranted the breach of privacy.

The same can be said about CSS for location data, e.g., contact tracing applications,[109] which so far would not be able to justify their existence via part 2 either. This does not mean that the surveillance will be criminalized, but practice indicates that it could be possible,[110] even if civil litigation is more likely.[111]

Like many types of existing surveillance, the ECtHR is not willing to directly require the removal of the techniques, most clearly seen with the techniques of entrapment earlier, which are allowed narrowly.[112] But, these must be implemented correctly, in a safety, security, and data pro-

[107] 43835/11, S.A.S. v. France [GC], § 114
[108] 20071/07, Piechowicz v. Poland, § 212.
[109] Lucie White and Philippe Van Basshuysen, "Without a trace: Why did corona apps fail?" (2021) 47(12) Journal of Medical Ethics E83.
[110] 38435/13, B.V. and Others v. Croatia, § 151.
[111] 25163/08, 2681/10 and 71872/13, Noveski v. the former Yugoslav Republic of Macedonia, § 61.
[112] 74420/01, Ramanauskas v. Lithuania [GC], § 51

tection context, which includes CSS.[113]

Violation by Existence

Questions could then arise as to how such surveillance systems could violate privacy of individuals by merely existing, such as through the medium.[114] Depictions and pictures of individuals are inherently protected by Article 8.[115].

This means that the individual must be protected against state and other private actors intruding on this right.[116]

As mentioned, this protection is not absolute, and no case law that relates directly to the protection outright without any essential criterion,[117] such as photos in the press, exists. Conversely, there is no case law which guarantees that any surveillance could be justified if sufficiently "privacy enhanced",[118] as the court leaves no room for exceptions if the surveillance is disproportionate and violates any degree of appreciation the state had or fails the tests above. This could be used to interpret Article 8 as never allowing privacy enhancing technologies to justify the measures. CSS systems like the CSAMD must therefore be analysed based on protecting the depiction of the individual, since this is the subject of the surveillance.

The question then becomes how far it reaches. The state must positively protect this right through criminal or civil law provisions.[119] It could mean that to use CSS, there should be legal safeguards that force Apple or other

[113] 58170/13, 62322/14 and 24960/15, Big Brother Watch and others v United Kingdom (Grand Chamber), § 362. See also Van Daalen (n 103) 12.

[114] This is further discussed in a more generic context, by *Van Der Sloot*, Bart Van Der Sloot, "A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle" (2018) 34(3) Computer Law & Security Review 539 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364917303849⟩ accessed 28 September 2023.

[115] 1874/13 and 8567/13, López Ribalda and Others v. Spain [GC], §§ 87-91.

[116] 40660/08 and 60641/08, Von Hannover v. Germany, §§ 50-53.

[117] 18068/11, Dupate v. Latvia, §§ 49-76.

[118] 30562/04 and 30566/04, S. and Marper v. U.K, § 125.

[119] 5786/08, Söderman v. Sweden.

companies to use state of the art encryption and demand local representatives that act as humans in the loop in their system.[120]

Defamation

The protection of individual reputation is also included in Article 8.[121] An attack of a certain level of seriousness must have occurred on the individual and it must have harmed the personal enjoyment for the right to respect private life.[122] This could be the planting of CSAM or false positives.

If CSS systems end up causing loss of reputation through the media or through companies/authorities themselves accusing the user, Article 8 can apply. The most important concept in this aspect is whether the loss of reputation was caused by user's foreseeable actions,[123] or if the loss of reputation was caused by a criminal conviction, which the court does not accept.[124]

From case law, this includes any part of the chain, and countries like the UK will allow this to be the basis for tort law or reimbursement law, with the company or state responsible as the potentially liable party.[125]

Finally, legislation which allows surveillance through any telecommunications or internet source will directly violate Article 8.[126] This includes any that could broadly secretly use CSS as a surveillance measure. This leads us to the next small section.

---

[120] Abelson and others (n 8).

[121] David Rolph, "Liability of internet intermediaries for defamation: beyond publication and innocent dissemination" in *Comparative Privacy and Defamation* (2016, 2020) vol 635; András Koltay, "Defamation on the internet: the role and responsibilities of gatekeepers" in *Comparative Privacy and Defamation* (2020); Kirsty Hughes and Neil M Richards, "The Atlantic divide on privacy and free speech" in *Comparative defamation and privacy law* (Cambridge University Press 2016).

[122] 76639/11, Denisov v. Ukraine, § 112.

[123] 25527/13, Vicent Del Campo v. Spain

[124] 76639/11, Denisov v. Ukraine [GC], § 98.

[125] Hughes and Richards (n 121).

[126] 72038/17 and 25237/18, Pietrzak and Bychawska-Siniarska and Others v. Poland, § 146.

State Surveillance

Because CSS systems may be part of secret state surveillance systems, similar safeguards as normal surveillance must be given.[127] These should include appeal processes and right to access. This is outside of what would be given through data protection rules, as access to its source code or similar is required to receive the process of a fair trial. To give an example of this, in an EU context, such data would not be covered by the GDPR, but instead the Law Enforcement Directive,[128] which limits the potential information which the individual would be able to obtain, and which requires the surveillance to fulfil a range of criteria, including authorisation.[129] This creates a discrepancy between national and supranational law, which has yet to be settled in case law.

CSS could take character of both strategic and individual monitoring, the first which focuses on searching for specific aspects in the surveillance through keywords and similar, while the latter is more akin to listening in.[130]

ECtHR practice, however, indicates that state surveillance via CSS without safeguards would be in violation of Article 8,[131] but there is one issue with this approach. Getting a case before a national court or the ECtHR requires

[127] 5029/71, Klass and Others v. Germany, § 36.

[128] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L119.

[129] Isadora Neroni Rezende, "Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective" (2020) 11(3) New Journal of European Criminal Law 375.

[130] 54934/00, Weber and Saravia v. Germany. See also Diego Zannoni, "GPS Surveillance from the Perspective of the European Convention on Human Rights" (2018) 8(2) European Criminal Law Review 294 ⟨https://www.nomos-elibrary.de/index.php?doi=10.5771/2193-5505-2018-2-294⟩ accessed 28 September 2023, 18.

[131] 4647/98, Peck v. the United Kingdom, § 59. See also the recent verdict in 72038/17 and 25237/18, Pietrzak and Bychawska-Siniarska and Others v. Poland, which affirms this practice.

that the state surveillance be *perceived or discovered*. If the CSS is hard to take to court, it becomes hard to prevent Human Rights Law violations. Leaving privacy, we take a brief look at Freedom of Expression and CSS.

4.3.3 Freedom of Expression

Freedom of Expression is self-evident from its literal meaning, but its complexity lies in how it should be understood depending on the context.[132] Article 10 applies to any medium,[133] but CSS systems like the CSAMD will not immediately impact the Freedom of Expression of any individual. Derived (chilling) effects seen in other types of surveillance systems will regardless of the intention lead to diminished rights,[134] especially freedom of speech[135] or theoretically any type of freedom.[136]
For Article 10 to have any effect, Article 11 must be adhered to as well.[137] We will come back to Article 11 in next section.

The three "tests"

Like the other ECHR rights discussed, Freedom of Expression is made in a positive manner. There exists a test which the courts have to take

[132] Ian Brown, *ONLINE FREEDOM OF EXPRESSION, ASSEMBLY, ASSOCIATION AND THE MEDIA IN EUROPE* (Report, Council of Europe 2013); Frederik J Zuiderveen Borgesius and Wilfred Steenbruggen, "The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust" (2019) 20(1) Theoretical Inquiries in Law 291 ⟨https://www.degruyter.com/document/doi/10.1515/til-2019-0010/html⟩ accessed 3 March 2024.

[133] 10572/83, Markt intern Verlag GmbH and Klaus Beermann v. Germany, § 26.

[134] Sometimes warranted for Freedom of Expression, see e.g., Gehan Gunatilleke, "Justifying Limitations on the Freedom of Expression" (2021) 22(1) Human Rights Review 91 ⟨http://link.springer.com/10.1007/s12142-020-00608-8⟩ accessed 14 February 2024.

[135] Amartya Sen, "Speaking of Freedom" [2002] The Little Magazine: Listen 9; Daniel J Solove, *Nothing to hide: The false tradeoff between privacy and security* (ISSN: 0009-4978 Publication Title: Yale University Press, 2011).

[136] Paul M Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52(6) Vanderbilt Law Review 1609.

[137] 52562/99 and 52620/99, Sørensen and Rasmussen v. Denmark, 2006, § 54. This creates a synergy that could quickly make any expanded surveillance system that ever remotely targets Freedom of Speech or Association illegal fast and could involve Article 8 under certain circumstances as well.

regarding whether Freedom of Speech can be suppressed.[138] This consists of three parts, which must be cumulatively fulfilled for the state to be able to justify violating Freedom of Speech: *Lawfulness of the interference (1), legitimacy of the aim pursued by the interference (2), necessity of the interference in a democratic society (3).* Failure at any stage will make the surveillance be in violation of Article 10.

1. Lawfulness of the surveillance system in interfering Freedom of Expression is attained with positively describing and implementing it in law, with the latter requiring precise wording and literal usage and meaning of the text.[139] The Court recognises that technology changes, and that wording can be made to be vague, but usage matters, and in this sense "what" the surveillance does.[140] This catches the issue of lawfulness; that it must be foreseeable for the user or individual whose Freedom of Expression is infringed. Future systems require proper implementation into law to not threaten Freedom of Expression through picture recognition of people and so on. This rules out any kind of private surveillance, which states would then have to protect its citizens against. It is not foreseeable for the individual that all their storage or other digital devices suddenly have CSS systems within them.

2. The surveillance must pursue a legitimate aim. This can be passed depending on the lack of constitutional protection of the system, or through popular movements, but they must be clear.[141]

3. The case law for the third test decides what should be done, not the wording as such. There must be a "pressing social need". Pressing here refers to an actual need and may not be twisted in practice or by other

[138] Gunatilleke (n 134).
[139] 24973/15, Cangi v. Turkey, §§ 39 and 42.
[140] 21279/02 and 36448/02, Lindon, Otchakovsky-Laurens and July v. France, § 41.
[141] 67667/09 and others, Bayev and Others v. Russia, §§ 64 and 83.

means through legislation,[142] though this does not make it indispensable. CSS could therefore be relevant during an insurrection or other emergencies or due to other extreme circumstances. Secondly, the assessment of the severity of the system must not lead to the assumption that it causes censoring.[143] Any kind of sanctions associated with the system must be proportional[144] and properly legislated and justified.[145] Thirdly, national courts can be part of the problem if they are not able to sufficiently and assess Article 10 in regards to this issue.[146]

This represents high bars for CSS to overcome to legitimately violate Freedom of Expression, and presents avenues which future lawsuits can take.

Next is ECHR Article 11 below, and its theoretical relationship to CSS.

4.3.4 Freedom of Assembly and Association

Freedom of Assembly and Association both should be understood literally, though their protection is quite wide in both applying to assembling and associating.[147] Like other articles, it sets out the right in Article 11, part 1, and then lays out exceptions in part 2, which are similar to e.g., Article 8 above.

CSS may be used to lawfully and unlawfully interfere with Article 11. This can be done through recognition of pictures, locations, people, or specific subjects. The aims for this kind of surveillance could be suppression of

[142] 6538/74, The Sunday Times v. the United Kingdom, § 59.
[143] 56925/08, Bédat v. Switzerland, § 79.
[144] 13444/04, Glor v. Switzerland, § 94.
[145] Bayev and Others v. Russia, supra, § 83.
[146] 23954/10, Uj v. Hungary, §§ 25-26.
[147]

Brown (n 132); Valerie Aston, "State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives" (2017) 8(1) ; Kalina Arabadjieva, "A Framework for Interpreting the Right to Freedom of Association of Workers and Trade Unions in European Human Rights Law" (Doctor of Philosophy, University of Oxford 2019).

political or non-political parties, specific public figures, or unions.[148]

Because of the nature of the surveillance, we focus on Freedom of Association. Article 11 and Article 10 are not in competition.[149] The freedom to associate with any political party is crucial[150] as is any other form of group.[151] To be included in the protection, the association must have a private character,[152] but the state cannot speculate in nationalising it on purpose to remove the Article 11 protection,[153] or in reality prevent any ineffective exercise of the right.[154] Article 11 states that any intervention with the right must "prescribed by law", pursue legitimate aims, and be "necessary in a democratic society". These are not defined in the same manner as Article 10. To be prescribed by law, the intervention of the Right of Assembly must be positively described in legislation, must be available for those affected, and must be foreseeable.[155] These present similar problems to what was seen in Article 10 for CSS.

Any CSS systems used for these purposes must be included in national legislation and the public must be clearly warned that they are able to use it to prevent assembly. Preventing assembly could be in the form of dissolving organisations (political, labour or otherwise) through identification and arrests, or milder economic sanctions.

The core point is that the CSS would be used for identification, as pictures contain metadata by themselves, or through the system, or clear location

[148] Aston (n 147); Ilia Siatitsa, "Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications" (2020) 102(913) International Review of the Red Cross 181 ⟨https://www.cambridge.org/core/product/identifier/S1816383121000047/type/journal_article⟩ accessed 3 March 2024.

[149] 20652/92, Djavit An v. Turkey, 2003, § 56

[150] 133/1996/752/951, United Communist Party of Turkey and Others. v. Turkey, 1998, § 25.

[151] 48848/07, Association Rhino and Others v. Switzerland, 2011 § 61.

[152] 7601/76 and 7806/77, Young, James and Webster v. the United Kingdom, 1979, Commission's report, § 167.

[153] 42117/98, Bollan v. the United Kingdom, 2000.

[154] 70945/11 et al., Magyar Keresztény Mennonita Egyház and Others v. Hungary, 2014, § 78.

[155] 39748/98, Maestri v. Italy [GC], 2004, §25 - 42.

or other data, and that they can contain elements that could link the user to the organisation that the state wants to quash. CSAMD and other CSS systems are capable of being re-purposed,[156] so that the system can look for these factors and through the same methods, alert a company (or the state using the system) which can then lead to further investigation and potentially litigate. Future systems are likely to be able to do this much easier and be designed for it.

Fortunately, the barriers which states would need to overcome to legitimise this surveillance are already high, as can be seen with the various tests presented in the last sections.

The next part discusses false positives and false negatives.

4.3.5 False negatives and false positives

CSS systems have two clear issues regarding results: false negatives and false positives.

False negatives[157] refers to the notion of the CSS system not detecting something. The ECHR does not directly discuss injustice or lack of enforcement outside of negative protection of rights, but it might not be unlikely that the ECtHR will decide on a case where someone else is put on trial for something which may have been caused by a false negative.[158]

False positives[159] are quite different and tightly connected to Article 6 of the ECHR. False positives should not be the basis of criminal investigations or proceedings. If this happens, the accused must therefore have a

[156] Abelson and others (n 8) 2.

[157] Alberto Lamas and others, "Human pose estimation for mitigating false negatives in weapon detection in video-surveillance" (2022) 489 Neurocomputing 488 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0925231221019159⟩.

[158] Ideally, false negatives should play no role and be filtered out before ever reaching courts, but it would be unwise to assume it cannot happen anyway.

[159] Dellinger and Hoffman (n 27) 75. See also Jerome C Wakefield, "False positives in psychiatric diagnosis: implications for human freedom" (2010) 31(1) Theoretical Medicine and Bioethics 5 ⟨http://link.springer.com/10.1007/s11017-010-9132-2⟩.

right to defend in person or through legal assistance through Article 6, § 3, c. This extends to the court system and the accused being able to question the authenticity of the evidence,[160] which is key to prove that the "positive" of the system is in fact a false positive. If the accused is not able to adequately question, comprehend or otherwise amount what is equal to any kind of defence against the false positive which the CSS system has produced, the trial cannot be considered fair and should lead to a retrial or even dismissal by the court. States making decisions based on false negatives is generally not unheard of.[161]

4.4 Client-side Scanning Outside of Human Rights Law

The examples taken in this chapter are in the context of CSS and Human Rights Law. Outside of this, CSS will likely also be covered by criminal or administrative law. In the next two pieces of legislation which I will look at, using CSS requires recruiting the platforms or service providers who host or manufacturer the infrastructure which CSS will be performed on. For both of these, the primary purpose is to prevent digital or online harms, particularly aimed at children,[162] hence their direct relevance with

[160] 50541/08, 50571/08, 50573/08 and 40351/09, Ibrahim and Others v. the United Kingdom, § 274.

[161] See classic themes like Colombia's False Positive problem, Juan Pablo Aranguren Romero, Juan Nicolás Cardona Santofimio, and Juan Ángel Agudelo Hernández, "Inhabiting Mourning: Spectral Figures in Cases of Extrajudicial Executions (False Positives) in Colombia" (2021) 40(1) Bulletin of Latin American Research 6 ⟨https://onlinelibrary.wiley.com/doi/10.1111/blar.13104⟩ accessed 3 March 2024; Daron Acemoglu and others, THE PERILS OF HIGH-POWERED INCENTIVES: EVIDENCE FROM COLOMBIA'S FALSE POSITIVES (NBER WORKING PAPER SERIES 2016); Rachel Johson, "The "False Positives" Scandal: Extrajudicial Killings and the Militarization of Domestic Security in Colombia" (Bachelor of Arts degree in International Studies, The University of Mississippi 2011); Rachel Godfrey Wood, Understanding Colombia's False Positives (Oxford Transitional Justice Research Working Paper Series 2009).

[162] There is an overlap between these two pieces of legislation, and the platform obligations given by the EU in its Digital Services Act, Regulation (EU) 2022/2065 of the

this chapter.

4.4.1 The Online Safety Act

The Online Safety Act[163] is a concrete example of legislation which may attempt to achieve its aims through mandating CSS. It has received royal assent and is current law in the UK. It was initially criticised for its very wide scope, and deliberately vaguely written[164] to give additional powers to the authority Office of Communications (Ofcom) who may delegate obligations to platforms and anything else that can be brought under the scope of the legislation. While not unknown to the UK, delegating the interpretation of how fundamental rights are understood in the context of CSS to private parties could potentially violate ECHR Article 6 and 8, as there is little in the legislation itself about how proportionality of the potential chat control or actions taken against citizens is understood.[165]

The Act does not only concern CSS but works with ideas like "proactive technology",[166] which can include CSS, or at least server-side scanning of user-generated or metadata.[167] Proactive technology is not just a possibility, it can be mandated by Ofcom in the aforementioned section, which is

European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L277. This specific issue is not further discussed in this thesis but serves as a potential additional angle to the CSS discussion. Other authors agree with this assessment, see Markus Trengove and others, "A critical review of the Online Safety Bill" (2022) 3(8) Patterns 100544 ⟨https://linkinghub.elsevier.com/retrieve/pii/S2666389922001477⟩ accessed 27 September 2023; Peter Coe, "The Draft Online Safety Bill and the regulation of hate speech: have we opened Pandora's box?" (2022) 14(1) Journal of Media Law 50 ⟨https://www.tandfonline.com/doi/full/10.1080/17577632.2022.2083870⟩ accessed 27 September 2023; Alexander Dittel, "The UK's Online Safety Bill: The day we took a stand against serious online harms or the day we lost our freedoms to platforms and the state?" (2022) 5 .

[163]Current version can be found here https://bills.parliament.uk/bills/3137, last accessed 11 December 2024.

[164]Dittel (n 162); Coe (n 162); Trengove and others (n 162).

[165]This could be regulated through other administrative legal rules or practices, but this should be clear in the legislation itself.

[166]See Section 137. Ofcom is supposed to define further in guidance.

[167]Section 137(6).

where a lot of the academic criticism has come from.

It is not clear whether Ofcom can or will roll back or otherwise mandate that the proactive technologies are stopped. This could force many types of systems with user-generated content, meaning anything from WhatsApp to Minecraft, to use CSS or server-side scanning, and which may never be changed or pulled back, making proactive surveillance the default on almost any type of system in which a user can create content. But this depends on what Ofcom decides to mandate, and whether the manufacturers of these systems chose to comply, and post-market surveillance by Ofcom. The potential Human Rights Law violations this Act presents should be clear from past sections of this chapter, as the Act does not attempt to clearly regulate the usage of CSS, something which several of the presented articles require to allow the violation of their rights. Secondarily, the Act confers any cybersecurity requirements to secondary legislation by not mentioning or requiring it at all, which can put both the subjects and even the systems themselves as risk, as was show in 4.2 in this chapter.

4.4.2 The Child Sexual Abuse Regulation

The proposed EU Regulation laying down rules to prevent and combat child sexual abuse[168] (CSA) has issues on which relate directly to the issues presented in this chapter. In its impact assessment of the proposed legislation, under its analysis of loss of fundamental rights, the European Commission claims on page 14 claims that CSS is "often the only possible way to detect it",[169] foregoing all other types of preventive and criminal

[168]Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (n 21).

[169]This kind of argumentation, with no references to any literature supporting it, can feel "Techno-solutionistic", John Gardner and Narelle Warren, "Learning from deep brain stimulation: the fallacy of techno-solutionism and the need for 'regimes of care'" (2019) 22(3) Medicine, Health Care and Philosophy 363 (ISBN: 0123456789 Publisher: Springer Netherlands) ⟨http://dx.doi.org/10.1007/s11019-018-9858-6⟩. The term im-

measures Member States can take against CSA.

The European Commission furthermore disregards and does not analyse the potential consequences either CSS or server-side scanning would have on cybersecurity and privacy, while they justify the victim's potential positive outcomes outweighing the negative of everyone else. The main tools of the Regulation are:

- Providers must conduct risk assessments (Article 3) and providers must mitigate risks (Article 4).
- Force app stores to prevent children from using inappropriate (not well defined) apps (Article 6), and force CSS or server-side scanning for all providers of communication services (Article 10) and backdoors, combined with potentially creating unlimited preservation of data if requested (Article 22).
- Add enforcement powers, which includes 6 percent of annual turnover or global income based fine (Article 35) and forcibly physically shutting servers down (Article 28 and 29).
- The creation of an EU Centre to facilitate technology and support providers and Member States, and have databases that are not well specified, without any requirements for its own staff and no assurance that EUROPOL will not *de facto* control or otherwise influence it.

Of further interest is especially Article 10, Technologies and safeguards, which in 10(1) states:

Providers of hosting services and providers of interpersonal communication services that have received a detection order shall execute it by in-

plies the proposal merely want to only solve a problem with a specific technology without regarding other factors.

stalling and operating technologies to detect the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable, using the corresponding indicators provided by the EU Centre in accordance with Article 46.

This follows the style of the Online Safety Act, in that the relevant authority can order hosts and providers to specifically look for CSAM, but here it can be done by installing freely provided technology (Article 10(2)).

It could clearly risk clashing with the Charter of Fundamental Rights of the European Union, or with the ECHR itself through Article 6 or 8. This is especially interesting since this is a Regulation, meaning it will have to fulfill the implementation into law requirements primarily, which it may not do.

4.5 Future Considerations

If CSS get implemented into our lives through all digital infrastructures, keeping check on their influence and consequences and what can be done to use them is of utmost importance, which means increased amounts of research into their actions upon the lives of those afflicted by them. This research should include judicial, cybersecurity and structural reviews, as well as more empirically based research through interviews of those that develop or are affected by them.

I hope that there will be an increased focus in the research on the down- or upsides, the costs of CSS, and the proportionality of the exercise. This question could be answered with an analysis focused on proportionality as a principle within law or philosophy, and would fit as an extension of existing research,[170] and the development of the EU CSA Regulation. A continuation of showing the impact on human rights of every kind by CSS

[170]Rosenzweig (n 25).

is needed as well.

4.6 Conclusion

In this chapter, I took a look at how CSS can be understood in a cybersecurity sense, the case of Apple's CSAMD, how CSS in general may violate or can be allowed within the ECHR via its case law, and how two new UK and EU proposals may show the worst side of CSS, despite their clear goal to fight against online harms and CSAM.

Because the literature surrounding CSS has not been clear, especially in an interdisciplinary context, this chapter provides a definition of CSS which both includes historical, current, and future ways to deploy such systems. I also included an abstract set of attacks, and an illustration which shows where each overarching category of attacks could occur within the ecosystem of CSS. These are Dataset Attacks, Hijacking or Manipulation Attacks, Communication Attacks, Entrapment, and Other downstream alterations. This provides a frame of reference for both cybersecurity and legal researchers who want to understand CSS.

Apple's suggestion for a CSS in the form of the CSAMD was inspected briefly;[171] a good attempt at a system which keeps most of the information and picture analysis private, until a threshold is met. There are far more elaborate and safer alternatives than the PSI and surrounding system which Apple chose for CSAMD, and this could in retrospect be considered the first major issue of the system.[172] Instead of relying on these safer alternatives, Apple decided to create an infrastructure which risk suffering

[171] We chose to not take Encrochat out as an example, as that specific case represents a situation where the entire infrastructure was compromised, and was more of a trap than a CSS, Van Daalen (n 103) 5.

[172] Abelson and others (n 8).

avoidable adversarial failures from the start.[173]

While this may change, this does not prevent the second issue of the system. I showed in this chapter that CSS like CSAMD will have the potential to not just violate one human right, but most likely $\leqq 2$ rights at the same time. CSS such as CSAMD may violate the EHRC Article 6 derived Right to Remain Silent and Not Incriminate Oneself, which could cause serious admissibility issues in courts, potentially preventing trials against criminals or otherwise disrupt legal systems. CSS also opens new possibilities for states to use entrapment.

Another right which could be violated is Article 8, which includes a right and protection of privacy. CSS will not pass the test of "necessary in a democratic society", exactly because these systems rarely will be proportionate in their infringements to their goals.

I discussed two more potential violations, which CSS may cause. This was Article 10, Freedom of Expression, and Article 11, Freedom of Assembly and Association. It was noted that CSS systems would rarely meet the thresholds to justify violating the rights, but what is important to acknowledge is the powerful ways which they could already do so. Surveillance systems seen in China are already capable of this.[174]

I finally commented on the Online Safety Act from the UK, and the EU proposed Child Sexual Abuse Regulation, who both may mandate CSS on providers of messaging and user-generated contents services, and that they may both lead to ECHR violations of Article 6 and 8.

---

[173] Struppek and others (n 43).

[174] Corinne Reichert, China reportedly scans tourists' phones by installing malware (Publication Title: CNET,, 2019) ⟨https://www.cnet.com/tech/mobile/china-is-reportedly-scanning-tourists-phones-with-malware/⟩; Lorand Laskai and Adam Segal, *The Encryption Debate in China: 2021 Update* (techspace rep, March, Carnegie Endowment for International Peace 2021) ⟨https://carnegieendowment.org/files/202104-Germany%7B%5C_%7DCountry%7B%5C_%7DBrief.pdf⟩.

4.6.1 Afterthoughts

Chapter four diverged significantly in terms of the law used from Chapter three, and the systems whose cybersecurity and design are in focus. CSS is purely software, though they can be implemented on all types of devices and services. The security for managing the analysis which these systems do should be heavily scrutinised, exactly because of the decisions or other outcomes these systems may end up providing. We learned that CSS are vulnerable through various points in its own infrastructure, meaning that very narrow and adequate safeguards must be implemented before it is used. In the case of what the case in chapter discusses, this is especially important. This is also a key point to keep in mind for the next section; not only is complexity a problem in cybersecurity, the same is the infrastructure, with distinct types of threats and issues at different points in any given process.

To further summarise, in this chapter we saw that Human Rights Law and security can create a synergy to improve both. While the former may put limits onto the latter, a well-designed system is able to fulfil the requirements put onto it. Protection of Human Rights requires the protection of those who are accused of something, and keeping the security high in this situation is paramount, both for the accused, but also for the potential victims, as not fulfilling criteria like self-incrimination, leading to admissibility issues, could thwart the efforts of authorities to prosecute. This multifaceted problem with both security (creating a secure enough system to effectively protect fundamental rights), and proper procedure (to prevent inadmissibility), and the national rules necessary (case law based), continue into the next section, but is also a lesson. While not new, it is but worth reflecting over in the context of CSS, especially considering its in-

creasingly vital role. CSS may become the standard with the inclusion of AI in most systems, and this chapter will therefore become more important going forward.

To end the chapter, I would like to answer the two questions posed in the introduction of this thesis.[175]

Human Rights Law understood by cybersecurity is an interesting combination, as they do not initially necessarily seem to have much to do with each other. The first is a system to protect fundamental rights, while the second is a computer scientific and engineering based field to protect security. But both echo "protect", and this is also how security understands Human Rights Law, as a security mechanism, but also as system requirements or compliance requirements, set by the public contract partners who have obligations to fulfil. Holistically and perhaps purposefully, Human Rights Law is something that cybersecurity wants to strive for and uphold, but it also sees it as an implicit or direct compliance measure.

CSS as understood by law is clearly seen as a means to an end, a tool to commit to surveillance and control. Interestingly, its intricacies can interact with many types of law,[176] and its problems can be contextualised in different aspects of Human Rights Law. This is can be clearly understood through its justification of its own existence being privacy (and therefore cybersecurity) enhancements, ease of use, constant logging and access control, all of which can have direct consequences if not implemented properly into national law, and if they violate or otherwise do not pass the tests posed by relevant courts.

[175] "How can this legal concept be understood in cybersecurity", and "how can these cybersecurity considerations be understood in law"?

[176] As it can directly be connected to Administrative, Criminal, Human Rights, and Private Law. The first two through what I have showcased in the chapters, while Private Law covers situations where additional litigation is necessary.

5 | Cyber Resilience in Supply Chain Cybersecurity: an EU Law Perspective

5.1 Introduction

Let me begin with a contrast to the chapters that preceded this one. Some researchers, such as *Taddeo*,[1] argue that cybersecurity should not always be a public good, even if cybersecurity concerns everyone's devices, critical infrastructure, and entertainment.

Taddeo further states: *"Framing systems resilience as public good used for the public interest may aggravate these risks by skewing public debate on this trade-off, misrepresent the level of security threats, the need for monitoring and surveillance, and the risks that these measures may pose to individual rights."*[2]

This view could be at odds with the rest of this thesis but is worth keeping in mind when engaging with the subject matter.

Before the advent of widely adopted digital infrastructure systems, the

[1] Mariarosaria Taddeo, "Is Cybersecurity a Public Good?" (2019) 29(3) Minds and Machines 349 (ISBN: 1102301909507 Publisher: Springer Netherlands) ⟨https://doi.org/10.1007/s11023-019-09507-5⟩.

[2] This statement contrasts what *Taddeo* then says in the following sentences regarding the constructive and useful potential of cybersecurity as a public good, see ibid 6.

biggest threats of information being stolen and by other means compromised was through the actions of its employees and from outside forces like spies and other intruders. By now, information as well as decisions can be altered and even physical manifestations can be seen from these infiltration attempts and successes. Stuxnet,[3] is an important and well known attack that included physical consequences. It succeeded because it executed a series of steps and actions and affected a monumental amount of physical and digital systems. This kind of stepping stone approach where one intrusion gives the attacker(s) access to an entire system of systems,[4] is like an attack on an entire supply chain or ecosystem. Successful attacks on entire systems are the greatest threats to any infrastructure supported by computers, whether civilian, commercial or military.[5] Because of the potential consequences if a provider of security, or the individuals links of the supply chains themselves, are compromised, one should be interested in uncovering the means which these companies can be held accountable.[6]

To this, on 16 March 2022, the European Commission launched a Call for Evidence for the future Cyber Resilience Act (CRA).[7] The specific call concerned itself with creating an Impact Assessment.

The proposal for the CRA[8] followed on 15 September 2022. I will in this chapter only work with this late 2022 version.

[3]Falliere, Murchu, and Chien (n 193).

[4]Shanto Roy and others, "Survey and Taxonomy of Adversarial Reconnaissance Techniques" [2022] ACM Computing Surveys 3538704 ⟨https://dl.acm.org/doi/10.1145/3538704⟩.

[5]Alessandro Creazza and others, "Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era" (2022) 27(1) Supply Chain Management 24.

[6]Keeping states accountable for allowing security failures to disrupt supply chains is a theme which this chapter does not focus on.

[7]See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en, last accessed 11 December 2024.

[8]Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final, 2022/0272 (COD).

This chapter sets out to answer how the CRA, which really will act more like general legislation regarding resilience in security, should be understood in terms of regulatory mechanisms, and how it would affect the cybersecurity of a case, here Supply Chain Cybersecurity (Supply Chain Security). This is done because of the knowledge which the economics of security as a field has generated since its inception,[9] and based on how existing European legal frameworks function. The latter is expressed with a comparative analysis of how the NIS1 Directive has been implemented in three jurisdictions through a Supply Chain Security lens.

A variety of research has been carried out on Supply Chain Attacks on an organisational, supply chain, and security level, but current legal measures are not well explored in the literature, with some exceptions.[10]

I will therefore comparatively analyse selected measures in several countries and the EU, both because of the diversity, but also because it gives a broad perspective and idea about how far we may be from properly regulating the risk of Supply Chain Attacks, as studying cybersecurity subjects is without a doubt complicated and interdisciplinary.[11]

To this, I want to add a more free and open-ended definition to Supply Chain Attacks on the basis of existing literature, which allows a broader and more inclusive understanding of the term.

After this, two practical examples of Supply Chain Attacks to provide a practical angle to the abstract problem are shown. The first occurred in 2020 without physical consequences to the company SolarWinds Inc.,

[9] Mazaher Kianpour, Stewart J Kowalski, and Harald Øverby, "Systematically understanding cybersecurity economics: A survey" (2021) 13(24) Sustainability (Switzerland); Axel Wirth, "The economics of cybersecurity" (2017) 51(Horizons) Biomedical Instrumentation and Technology 52; Mazaher Kianpour, Stewart James Kowalski, and Harald Øverby, "Advancing the concept of cybersecurity as a public good" (2022) 116(January) Simulation Modelling Practice and Theory (Publisher: Elsevier B.V.).

[10] Eldar Haber and Tal Zarsky, "Cybersecurity for Infrastructure: A Critical Analysis" (2017) 44(2) Florida State University Law Review.

[11] Jacob, Peters, and Yang (n 195); Suryotrisongko and Musashi (n 167).

which provides systems for managing software and other products. One difference between it and Stuxnet was that this affected everything from public authorities, including foreign intelligence of several countries, to wealthy private companies. As of the time of writing, it is not entirely clear what the purpose or the gains of the attack was.[12]

The other example is the Kaseya Ransomware Attack,[13] where another type of security structure was compromised and used to inject ransomware into the users. Unlike the SolarWinds Inc. attack, it was not caused by an equally sophisticated payload, but by a vulnerability that was discovered earlier. Its effect on commercial and public enterprises, as well as its clear physical consequence by disabling card payment systems in 100s of physical stores[14] makes it worth considering as an alternative to sophisticated attacks, which can cause the same type of damage.

I recognise that there already exists EU legislation on cybersecurity through the NIS1 directive[15], the NIS2 directive[16] and the Cybersecurity Regulation[17], the latter focused entirely on EU institutions. While the spirit and the idea behind the NIS1 directive is admirable, it does not put proper security into hard law, but leaves it for guidance and certifications and

[12]Other than the US Department of Justice confirming the compromise of their mailing environment, see https://www.justice.gov/opcl/department-justice-statement-solarwinds-update, last accessed 11 December 2024.

[13]https://www.zdnet.com/article/kaseya-ransomware-attack-what-we-know-now/, last accessed 11 December 2024.

[14]https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant, last accessed 11 December 2024.

[15]Directive 2016/1148, concerning measures for a high common level of security of network and information systems across the Union, [2016] L 194/1.

[16]Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), [2022] OJ L333/80. It will not be analysed in detail this chapter, as its implementation is ongoing. For more, see Niels Vandezande, "Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor" (2024) 52 Computer Law & Security Review 105890 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364923001000⟩ accessed 24 May 2024.

[17]Regulation 2019/81 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU)No 526/2013 (Cybersecurity Act), [2019] L 151/15.

other soft law measures, without enforcement regimes worthy of how central and important security is.[18] Furthermore, the NIS1 directive does not implement the practical tools and procedures needed to make systems resilient,[19] instead merely focusing on strategies, the Cooperation Group, security incident response network, and appointments of national competent authorities.[20] On the other hand, the Cybersecurity Regulation represents a good starting point as to how the best security possible can be established,[21] and useful concepts being put into hard law.[22]

I build on the literature within cybersecurity and law that applies to digital technologies with additional concepts from safety engineering, a branch which traditionally was connected to physical equipment or structures which can harm or pose a safety risk to legal or physical entities, finance, health, or otherwise. But as the EU itself has already recognised that[23] safety can be directly influenced by security,[24] which means we must have these concepts included.[25]

This furthermore sets the scene for answering the two questions posed in

[18]And with glaring issues from the get go (Sandra Schmitz-Berndt and Stefan Schiffner, "Don't tell them now (or at all)–responsible disclosure of security incidents under NIS Directive and GDPR" [2021] 35[2] International Review of Law, Computers and Technology 101 [Publisher: Taylor & Francis] ⟨https://doi.org/10.1080/13600869.2021.1885103⟩) in the form of very unclear reporting requirements.

[19]See also Tobias Liebetrau, "Problematising EU Cybersecurity: Exploring How the Single Market Functions as a Security Practice" (2024) 62(3) JCMS: Journal of Common Market Studies 705 ⟨https://onlinelibrary.wiley.com/doi/10.1111/jcms.13523⟩ accessed 24 May 2024.

[20]See the NIS1 directive, Art 1(2).

[21]The empowerment of ENISA in Chapter II is one good example. On the contrary, see Myriam Dunn Cavelty and Max Smeets, "Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority" (2023) 30(7) Journal of European Public Policy 1330 ⟨https://www.tandfonline.com/doi/full/10.1080/13501763.2023.2173274⟩ accessed 24 May 2024.

[22]Art 46 being an example of a proper development of enforceable certifications, but these may conflict with the ideas in this chapter.

[23]See page 10 in the 'Guidance on Cybersecurity for medical devices' by the MDCG, https://ec.europa.eu/docsroom/documents/41863, last accessed 11 December 2024.

[24]Also noted and expanded upon in Anderson (n 3) 1044 - 1045.

[25]This is not part of the traditional safety to security discussion, as this involved the traditional meaning of security, malicious actions, versus well intended Leveson (n 163) 182. But cybersecurity does contain this element as well, so it is still worth reading.

the introduction.[26]

In this chapter, I do not attempt to solve or otherwise find the ideal type of regulation to end Supply Chain Attacks. It is instead an attempt to highlight the dangers and potential with the two cases, and then show what concrete law would apply in specific jurisdictions. In this sense, I do not analyse individual agreements between states and cybersecurity providers or other relevant contractors, which in practice could prevent or otherwise are vital to stop Supply Chain Attacks.[27] Similarly, I will not discuss decrees, soft law, or procurement issues or solutions.

The chapter is structured as follows:

Section 5.2 introduces the relevant EU rules, Section 5.3 analyses the CRA proposal, Section 5.4 briefly introduces the Supply Chain Security case of the chapter, and Section 5.5 dives into examples of Supply Chain Attacks, and narrowly focuses on the implementation of NIS1 in three different legal systems. 5.5 also includes commentary on how the CRA applies to Supply Chain Security, followed by a small commentary on NIS2. finally, Section 5.6 contains the conclusion of this chapter.

5.2 Law and Guidance

5.2.1 Resilience

Briefly before discussing the legal aspects, we must first agree on and understand the central term to the CRA and the title of this chapter.

Resilience as a concept consists of the elements of a system (be it small or massive) which allow *fault detection, fault tolerance, error recovery and*

[26] "How can this legal concept be understood in cybersecurity," and "how can these cybersecurity considerations be understood in law"?

[27] This would be ideal to do in future work through qualitative analysis however.

failure recovery.[28] This constitutes the core of what the CRA is supposed to do, and to understand resilience, you must understand every other part of its being and all types of recovery and detection. None of these are easy, and rely on classic engineering ideas such as redundancy, logs, backups and so on.

Implementing resilience is not the same as proposing its existence, akin to calculating risk and actually managing it. The choice of tools depend on which type of defence is needed.[29] What matters is whether the resilience is anchored by the practical failure tolerance, recovery, and preventive systems; whether there is redundancy in the form of backup servers matters little if the adversary also has hit them with ransomware, or if they keep on initiating attacks on the basis of errors in IoT equipment which the manufacturer is never going to patch. It is therefore paramount to understand resilience as a constant level of readiness, not as an attribute that can be given to a system and then abandoned.

Additionally, any notion of resilience in an individual system will fail if the supply chain of security, e.g., security service providers, ISPs, physical security, are compromised by adversaries. Resilience cannot be maintained in those situations, because of the increased risk of compromises, or the lack of manageable failure recoveries due to the risk the other parties of the chain pose. This makes the concept of supply chains in cybersecurity intrinsically important to resilience of any digital system, and especially if these systems can create safety failures that can cause injuries.

Resilience as a value in safety and security engineering is not positively and literally dealt with in legislation. It has traditionally been left up to the private or public parties, who must realise it, being encouraged by the potential of lawsuits and responsibility for damages caused by not having it,

[28] Anderson (n 3) 251 - 252.

[29] *Anderson* makes an overview of the general issues, ibid 252 - 258.

or through guidance by relevant authorities. Exceptions to this are showcased in Section 5.5 in this chapter, as there is now EU legislation which gives more explicit commands regarding parts of resilience. The CRA will be part of this, but unlike those examples, exists as product legislation.
Despite this, engineers seem to also have affected some lawmakers and legislators, as there are special considerations taken in regards to supply chains and therefore also Supply Chain Attacks.[30] Additionally, voluntary relationships between states and companies responsible for supply chains or cybersecurity exist but cannot replace the needs for possible hard legal responses to attacks and failures on whole systems.[31]
In the following section, I will take a close look at relevant European Legislation, which is necessary to understand before focusing on the CRA.

5.2.2 European Law

The EU can only control certain areas because they are limited by competence.[32] Unless the competence is shared, or fully given to the EU, it cannot legislate or otherwise control or mandate topics for the member states.
But they have provided an array of guidance as well as legislation which is relevant to the CRA, cybersecurity, and Supply Chain Security at large.

Cybersecurity Legislation

The most well-known and used security legislation, legislation that directly attempts to impose security obligations, in the European Union, is

[30]While not the focus of the paper and only lightly commented on in Section 5.5.5, they do exist, and deserve additional analysis elsewhere.

[31]J Shackelford, Scott Russell, and Jeffrey Haut, “BOTTOMS UP: A COMPARISON OF "VOLUNTARY" CYBERSECURITY FRAMEWORKS” (2016) 16 45; Robert Gyenes, “A Voluntary Cybersecurity Framework Is Unworkable- Government Must Crack the Whip” (2014) 14(2) Pittsburgh Journal of Technology Law and Policy 293.

[32]See Article 4.2 and 6 of the Treaty of the Functioning of the European Union, C 326/47.

the NIS1 Directive.[33] It is a directive and therefore requires implementation[34] in each European Member State, which means there will be some divergence and legal fragmentation across the Union.

Before I explain how this is further relevant to the security of supply chains, further justification as to whether it can be applied to them or not is necessary. This is done in national law through implementation. The NIS1 directive does not mention Supply Chain Attacks or adversarial attacks, but it is still relevant, because it sets up the infrastructure for the protection against them. For the Directive to apply to Supply Chain Security, the supply chain must contain companies or public entities that are "operators of essential services" defined in Article 4(4) and defined by the Member State in Article 5(2). Article 4(4) requires that they furthermore work within Annex II, which has seven broad categories, being:

1. Energy
2. Transport
3. Banking
4. Financial market infrastructures
5. Drinking water supply and distribution
6. Health
7. Digital infrastructure

This leaves out providers of the security of these infrastructures, so cases like the Kaseya Ransomware Attack and the Sunburst Backdoor. Firstly,

[33] Directive (EU) 2016/745 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L194/1.

[34] For progress of the concrete implementation, see https://digital-strategy.ec.europa.eu/en/policies/nis-transposition, last accessed 11 December 2024. There is no site that updates progress on NIS2 yet as of the time of writing.

because both companies are based in the US, and secondly because they are not included in any of these categories. However, it may be possible to include them in an expanded version of the seventh category, but this is only possible through national law.[35]

The first six categories can be understood literally, but digital infrastructure should be explained. The Directive sets out to cover IXPs (Internet Exchange Points), DNS (Domain Name System) service providers and TLD (Top Level Domain) name registries. But there is nothing in the Directive that does not allow a Member State to include many more companies into their definition of "operator of essential services". An expanded definition of this could therefore be ISPs (Internet Service Providers), SoMe providers, major security providers and more, and this would allow any Member State to force the NIS1 Directive to apply to those that are often responsible for the mitigation of Supply Chain Attacks. I will note whether any of the two Member States or the UK have done so in their implementation of the Directive later in this chapter.

The second piece of security legislation in the EU I will focus on,[36] is the Cybersecurity Act.[37] Its title is deceptive, as it instead expands the powers of The European Union Agency for Cybersecurity (ENISA) and the initial process of cybersecurity certification.[38] The Act has no literal details on Supply Chain Attacks or adversarial attacks in general.

[35]These examples are in Section 5.5.1.

[36]This act deserves its own paper for further security analysis, but it is relevant to discuss which influence it has the practical and real measures to mitigate Supply Chain Attacks.

[37]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L151/15.

[38]See additional analysis by Irene Kamara, Misaligned Union laws? A comparative analysis of certification in the Cybersecurity Act and the General Data Protection Regulation (2021); Federica Casarosa, "Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act" (2022) 3(1) International Cybersecurity Law Review 115 ⟨https://link.springer.com/10.1365/s43439-021-00043-6⟩.

Initially, ENISA does not gain any powers that would transform it into a regulatory authority, it instead keeps its position as an advising and guiding institution.[39] There is therefore no central overarching and controlling "big brother" when it comes to the regulation of security in the EU. There are however national regulators, but they are quite limited as to when they can enforce compliance. For the national authorities, their only action is to withdraw certification from legal or physical entities regarding their software.[40] They are not capable of anything else in a direct and effective sense.[41] Because of this, no further comment on any practical or national consequences regarding the mitigation of Supply Chain Attacks by the Cybersecurity Act will be done in this chapter, and because the certification scheme is (yet) not implemented or relevant on a European level.

However, as indicated by the Act, ENISA publishes guidance and opinions and is supposed to be the central knowledge facilitator regarding security, and I will therefore mention some that are highly relevant to Supply Chain Attacks.

Finally, a new proposal for the Cyber Solidarity Act[42] was recently unveiled, which will create emergency mechanisms in the event of broad adversarial or Supply Chain Attacks, both at a national and a European level.[43]

[39] See Art 3 and 4 of the Act.

[40] See Art 56(8).

[41] This depends on whether one views certification as an effective measure to increase security and prevent Supply Chain Attacks, or whether one prefers hard legal remedies and obligations.

[42] Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, COM(2023) 209 final, 2023/0109 (COD).

[43] This too deserves its own paper, as it must scrutinised from a cybersecurity perspective in terms of its legal ideas, versus how response teams work in practice.

Guidance

To support the role of Supply Chain Attack prevention in the regime of the Directive, ENISA frequently publishes a threat landscape, and have their own taxonomy for the Supply Chain Attacks, which is less abstract and highly practical.[44] They are based on empirical information from incident reporting across the EU. Most of the content is therefore related to practical considerations and types of attacks, but they do include a list of recommendations. They refer to fulfilling ISO and other standards, Google's End-to-End Framework for Supply Chain Integrity[45] and other government recommendations.[46] Most of the technology and abstract ideas and security concepts that enable defences against Supply Chain Attacks are developed by academic researchers or other individuals,[47] and it would suit ENISA to follow suit and use more time developing the technical standards of their own, instead of referring to existing commercial ones. This may happen with the certification structure from the Cybersecurity Act.

Regardless, this guidance makes an especially crucial point that we need to keep in mind, which is that not everything is a Supply Chain Attack.[48] It can appear to be so, but it may be caused by design deficiencies or unpredictable behaviour of the software, or it may simply be an adversarial attack that does not target links of the supply chain. A special methodological limitation is further added, in which a Supply Chain Attack that succeeds to infiltrate for example a service supply chain, like management

[44]https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, last accessed 11 December 2024.

[45]https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html, last accessed 11 December 2024.

[46]Like one written for the US government, which is generic and yet recommended by ENISA, see https://d3fend.mitre.org/ *A knowledge graph of cybersecurity countermeasures*, last accessed 11 December 2024.

[47]EGabriella Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton University Press 2013).

[48]P. 26.

software, but has targeted outdated versions of the software where users are not paying or part of the chain that the original manufacturer controls, will *not* be considered a Supply Chain Attack.

Other

Other legislation will have security requirements included through wording or through guidance. GDPR is an example of the first, product legislation like the MDR[49] and the AI Act[50] is the latter. The first works with the term "state of the art",[51] which refers to security, and therefore has vague requirements that are at least supposed to prevent abuse or leakage of personal data, but not mitigation of the Supply Chain Attack explicitly. Like any product legislation that includes digital infrastructures, the MDR has guidance issued by its central authority that should be followed. There is no literal legal requirement, but it is heavily encouraged or even forced if caught before certification and release of the device.[52]

I can now move on to the CRA proper.

5.3 The Cyber Resilience Act Proposal

As of the time of writing this chapter, there have been a series of negotiations which resulted in three different versions of the CRA from the

[49]Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. Not mentioned in the text, but part of the requirements for functioning in its Annex I.

[50]Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM/2021/206 final. See specifically Art 15.

[51]Preamble 83.

[52]See "Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR", https://ec.europa.eu/docsroom/documents/37581, last accessed 11 December 2024.

European Parliament,[53] The Council of the European Union, and the European Commission.[54] But because these are the basis of negotiation, and not predictable as to which will prevail, and by which means, we therefore focus on the original proposed text from 2022.

5.3.1 Contents and Overview

After the initial impact assessments and hearings, the Horizontal Framework solution was chosen.[55] This is also seen in its status as Act, and not an EU Directive. It allows the CRA to function in its literal form, instead of risking legal fragmentation.

The CRA is designed as most product legislation, with the structure of General Provisions (Chapter I), Obligations of Economic Operators (Chapter II), Conformity of the Product With Digital Elements (Chapter III), Notification of Conformity Assessment Bodies (Chapter IV), Market Surveillance and Enforcement (Chapter V), Delegated Powers and Committee Procedure (Chapter VI), Confidentiality and Penalties (Chapter VII), and Transitional and Final Provisions (Chapter VIII). This mirrors legislation like the MDR in structure, and type of authorities.

I will now look at one of the central elements of the functioning of the CRA, the purpose, which is relevant to its application on Supply Chain Security.

[53] For a current version from their side, see https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act?sid=7101, last accessed 11 December 2024.

[54] For the Council's current version, see https://www.consilium.europa.eu/en/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/, last accessed 11 December 2024.

[55] CRA proposal, p. 8 - 9.

The Purpose

Before the release of the proposal for the CRA, the European Commission set a range of purposes for the new legislation, which are not mentioned in the text.
The three purposes are:[56]

1. To enhance and ensure a consistently elevated level of cybersecurity of digital products and ancillary services, secured throughout their whole lifecycle proportional to the risks.

2. Match users to fit the security properties of products with their needs, which should protect users from insecure digital products and ancillary services and incentivise vendors to offer more secure products.

3. To improve the functioning of the internal market by levelling the playing field for vendors of digital products and ancillary services.

This sets up an equal split between market considerations and user and/or consumer protection. Users are not alike, thus perhaps specifying and protecting consumers explicitly would be beneficial, but this may also be ideally done in practice by consumer rules in general.
Different parties have different interests, and this is not expressed well in these purposes - to ensure the first purpose, the different interests of both private and public users should be considered. Private parties may want the highest cybersecurity possible and have little understanding towards mechanisms which seek to breach this level of security for other purposes than their own interests.[57] Conversely, public users may want

[56] See page 2 - 3 in the Call for Evidence. These purposes are not quoted but paraphrased.

[57] Note that their own interests could be profits, hence they may also be focused on the cheapest solution possible. But "cheap" does not mean poor security, as good security means less issues long-term.

high cybersecurity in specific areas, such as surrounding military or other public authorities, while insisting on back doors and every means possible to breach purpose one, against its own citizens through mass surveillance and similar activities. This split can be seen in practice in Data Protection, where the GDPR explicitly does not regulate military,[58] and criminal investigation related data processing.[59]

In practice, the purpose is then expressed in subject and scope of the CRA:[60]

"(a) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;

(b) essential requirements for the design, development, and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;

(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;

(d) rules on market surveillance and enforcement of the above-mentioned rules and requirements."

This should be understood together with Article 2(1):

"This Regulation applies to products with digital elements whose intended, or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network."

Article 1 gives us a clear split in priorities of the CRA between regulat-

[58] See Article 2(2)a of the GDPR.

[59] See Article 2(2)d. For specific rules on this, see Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L119/89.

[60] Article 1 of the CRA.

ing cybersecurity requirements for the products in a and b, regulating the action/inaction of manufacturers in c, and market surveillance and enforcement in d. Article 2(1) narrows the type of products which are to be regulated to anything with digital elements, which now or later can have a direct/indirect logical or physical connection to another device or a network.

From this, one can clearly see the Supply Chain Security context; the CRA applies to the products everywhere in the chain at once. Anything from IoT or cyberphysical systems on the bottom, actuators and sensors in robots, control systems in the middle of the chain, and the computers which those that direct and administrate the systems use, will be regulated by the CRA.[61]

Overall, this gives us the outline of what the CRA will regulate, and glimpses of how it will do it. But this does not tell us how it will enforce or make its purpose into reality - this will be the focus below.

5.3.2 Regulatory Mechanisms and Structure

In this section, I analyse the enforcement structures of the proposal.

Compliance

Compliance is dictated by the culture, behaviour, and place in society of the subjects which you aim to regulate.[62]

[61] I will return to this in Section 5.5.4.

[62] Daniel Peat, "Perception and Process: Towards a Behavioural Theory of Compliance" (2022) 13(2) Journal of International Dispute Settlement 179 ⟨https://academic.oup.com/jids/article/13/2/179/6439208⟩.

Security is implemented everywhere, which means the compliance of rules surrounding it must depend on its context.[63] In reality, military intelligence members have smartphones, medical equipment may still use Windows XP, social media platforms use poorly implemented and easily attackable ML models and so forth.[64] Adjusting expectations from assuming we can divide usage into different levels may therefore not be relevant, even if the comparison between critical infrastructure to consumer devices would normally entail different levels of security, it does not have to. Considering the amount of devices that are used by consumers, it should be at least equal, as devastating attacks on such devices in bulk may even be analogous to attacking critical infrastructure.

The CRA envisions several tiers of compliance. The first is a requirement of fulfilment for complying before placing the product onto the market in Article 5, combined with an extensive number of obligations for the manufacturers in Article 10. Secondly, special requirements are set for Critical Products with Digital Elements in Article 6, which includes many types of software and hardware[65] used in all supply chains.[66]

[63] Mark A Harris and Ronald Martin, "Promoting Cybersecurity Compliance" in Ismini Vasileiou and Steven Furnell (eds), *Advances in Information Security, Privacy, and Ethics* (IGI Global February 2019) ⟨https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-7847-5.ch004⟩ accessed 1 March 2024; Jennifer M Pacella, "The Cybersecurity Threat: Compliance and the Role of Whistleblowers" (2016) 11(1) Brooklyn Journal of Corporate, Financial & Commercial Law.

[64] Ahmet Duzenci, Hakan Kitapci, and Mehmet Sahin Gok, "The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior" (2023) 13(15) Applied Sciences 8731 ⟨https://www.mdpi.com/2076-3417/13/15/8731⟩; Charlette Donalds and Kweku-Muata Osei-Bryson, "Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents" (2020) 51 International Journal of Information Management 102056 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0268401218312544⟩ accessed 1 March 2024; Derek Mohammed, "Cybersecurity Compliance in the Financial Sector" (2015) 20(1) ; Pacella (n 63); Maranda McBride, Lemuria Carter, and Merrill Warkentin, *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies* (Prepared by RTI International – Institute for Homeland Security Solutions under contract 3-312-0212782, 2012).

[65] For the full list, see Annex III of the CRA.

[66] Additionally, overlaps with the AI Act and the future Machinery Regulation are dealt with in Art 8 and 9.

This then follows various paths which involve notified bodies, as there are both Class I and Class II products.[67] For all devices and systems, there will be a presumption of compliance,[68] which manufacturers must make into practice[69] to get the CE marking.[70]

The structure of notified bodies depend on the national system, as the Member State is free to either choose one or several notified bodies[71] to handle the technical and procedural aspects of the process, but the last steps always involve the notifying authority,[72] who, like in other product legislation, controls the notified bodies.

Compliance cannot be reached fully with certificates, as these are not reviewed or otherwise renewed or controlled at a rate which breeds confidence.[73] This does not diminish their value in creating or inspiring a strong basis for which hard legal rules to create, and for which reasons. They can be made in a way where their status is reviewed, making them valuable tools, if not an active part of the compliance system, but their issues must stay as an active consideration at all stages in the process.

This is the case for the CRA, which puts the CE mark in centre together with Annex I and IV, and then may require additional private standards fulfilled on top.[74]

Enforcement

Due to the central role security has in the lives of most people, either directly in their pockets or through companies or the Member States them-

[67] Annex III. And for critical products with digital elements, special procedures exist, see Art 24(3).

[68] Art 18.

[69] They must start this process with a conformity assessment, see Art 24.

[70] Art 20.

[71] Art 29, 30, 31, and 37.

[72] Art 26 and 27. These can take the role of Market Surveillance Authorities.

[73] Anderson (n 3).

[74] These can be included as the "harmonised standards", see Art 3(34), found in Art 18(1).

selves (security in their systems), parallels to GDPR should be quite adequate. This implies strong enforcement, and such enforcement is only possible through similar mechanisms.

In practice, the CRA does so through its Market Surveillance Authorities, who may be notifying authorities as well if the Member States decides them to be, and who must continuously monitor the market and the products which are covered by the CRA. This is a task which is by itself massive, but it only increases when the specialised rules on significant cybersecurity risk are included.[75] Market Surveillance Authorities also have the power of "sweeps", which mimic existing powers in other product regulation in the EU.[76] They also possess powers which allow them to withdraw[77] or otherwise remove the products from the market.

The problem is enforcement as such. I have no knowledge of the powers, staffing, and additional national law, such as public legal principles, which allow the Member States to properly regulate the cybersecurity across the EU. The authorities may possess the right powers, but it may be unable to understand what they survey and find in their post-market surveillance, may not have the right staff, rights in the national legal system, and equipment to stop distribution physically and digitally, and finally, there is no mechanism to make information for their practice public across the EU.

The last risk comes from the all-encompassing role which Supply Chain Security has; enforcement must both happen at the lowest, middle, and highest levels of the chain at the same time. Any elements which could be touched by faulty systems, and which could for example be considered significant cybersecurity risk, would need separate assessments, potentially

[75] Art 43, 45, 46 and 47. The last two are on Member State or Commission level but require the authorities to cooperate in practice.

[76] Art 49.

[77] See Art 43(1) and 43(4), and equivalents in Art 45 and 46. Notified bodies can also withdraw their certification, see Art 37(5).

making entire supply chains, and anything they affect into subjects of potential enforcement.

The size and scale of this seems wider than any of the individual Market Surveillance Authorities may be able to handle, and will depend on cooperation between authorities,[78] national cooperation, and cooperation between the EU and its Member States. The latter two are unclear in this draft, they may either become reality through Article 43, 44 and 45, or through informal collaboration with private parties and Member States and the EU.[79]

With this characterisation of the CRA, and its various problems and tools to regulate cybersecurity, I move on to the case of Supply Chain Security and its relationship with the NIS1 Directive.

5.4 Case: Supply Chain Cybersecurity

In Special Publication 800-37,[80] the US authority National Institute of Standards and Technology defined supply chains as:

Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

I note that the cybersecurity of digital, even more so than physical supply chains, can be characterised by:

1. Excessive market tipping and monopolies.

[78] Art 48.

[79] In practice, this may be established or run in cooperation with ENISA, and on the legal basis of the EU Cybersecurity Act and the proposed Cyber Solidarity Act. I cannot discuss this in further detail in this chapter, but it may be worth exploring in future work in the context of Supply Chain Security.

[80] https://csrc.nist.gov/pubs/sp/800/37/r2/final, last accessed 11 December 2024.

2. Network effects.

3. Durability impacting complexity arising from software interdependencies.

4. Disintermediation of alternatives.

5. Lack of transparency.

First point is the notion of increased use of specific operating systems, security systems or other specialised software or service, which then leads to monopolies or oligopolies in certain fields.[81]

Second point stipulates the influence that products which have high user bases may cause. Network effects are well documented in cybersecurity,[82] and they are further exponentially scaled in supply chains, as the security providers that most use will, in turn, create greater insecurity if they are compromised both on a hardware and software level.

The third point shows the great weakness of the first two. The complexity, or the lack thereof depending on the supply chain, will change and potentially lead to further weaknesses, and no standards or cybersecurity rules currently account for this.[83] The notion that software complexity can both be an advantage and disadvantage seems extremely important to consider, when any supply chain adds layers upon layers of interconnected and act-

[81] Nick Economides and Ioannis Lianos, "Restrictions on Privacy and Exploitation in the Digital Economy: A Competition Law Perspective" [2019] CLES Research Paper Series. The following source ads a historical but crucial perspective Charles Duan, "OF MONOPOLIES AND MONOCULTURES: THE INTERSECTION OF PATENTS AND NATIONAL SECURITY" (2020) 36(4) Santa Clara High Technology Law Journal 39.

[82] Zahid Rashid, Umara Noor, and Jörn Altmann, "Network Externalities in Cybersecurity Information Sharing Ecosystems" in Massimo Coppola and others (eds), *Economics of Grids, Clouds, Systems, and Services* (Series Title: Lecture Notes in Computer Science, Springer International Publishing 2019) vol 11113 ⟨http://link.springer.com/10.1007/978-3-030-13342-9_10⟩ accessed 1 September 2023; Johannes M Bauer and Michel JG Van Eeten, "Cybersecurity: Stakeholder incentives, externalities, and policy options" (2009) 33(10-11) Telecommunications Policy 706.

[83] Christoph Neubert and others, *There is no Software, there are just Services* (Irina Kaldrack and Martina Leeker eds, 2015) 49.

ing software and hardware. Such a lack of rules may end up negatively impacting the durability and the safety of the supply chain if collaborators or links in the chain are unsuitable.[84]

The fourth point relies on poor competition legislation and competition in practice. If there is no way to easily explain and understand what software and service solutions are the most adequate for a specific supply chain, then myriads of vulnerabilities and failures become close to inevitable. This goes into issues in both competition and public procurement in national jurisdictions.[85]

Finally, the fifth point relates to the issue of the lack of transparency. Public accountability and clear evidence for auditing and future lawsuits should demand this, both *ex ante* and *ex post* for when the failures do occur. Furthermore, the very nature of any supply chain also causes reduced visibility, understanding, and control further into the system.[86]

These factors may have led to a highly oligopoly-like landscape.[87]

[84]Richard J La, "Role of network topology in cybersecurity" (IEEE December 2014).

[85]There is currently no literature on supply chain cybersecurity competition law issues in the legal community.

[86]Jon Boyens and others, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (techspace rep, National Institute of Standards and Technology 2021) ⟨https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf⟩.

[87]Regulating this may become problematic, see past encryption history for this, JH Ellis, "THE HISTORY OF NON-SECRET ENCRYPTION" (1999) 23(3) Cryptologia 267 ⟨http://www.tandfonline.com/doi/abs/10.1080/0161-119991887919⟩; ZIsadora Hellegren, "A history of crypto-discourse: encryption as a site of struggles to define internet freedom" (2017) 1(4) Internet Histories 285 ⟨https://www.tandfonline.com/doi/full/10.1080/24701475.2017.1387466⟩; Patrick D Anderson, "Review of *Crypto Wars—The Fight for Privacy in the Digital Age: A Political History of Digital Encryption*" [2021] Cryptologia 1 ⟨https://www.tandfonline.com/doi/full/10.1080/01611194.2021.2002977⟩; Milana Pisaric, "Communications Encryption as an Investigative Obstacle" (2022) 60(1) Journal of Criminology and Criminal Law 61.

5.5 Supply Chain Attacks

The following section discusses the idea of Supply Chain Attacks on a terminological level, and suggests a unique way to conceptualise it.

The US Committee on National Security Systems, in CNSSI No. 4009,[88] define Supply Chain Attacks as:

"An incident where an adversary exploits vulnerabilities in the product or service supply network of the intended target."

In 2011, in a report made on behalf of Microsoft,[89] four key areas were identified and deemed to be important to cyber supply chain management for states; *risk-based approach, transparency, flexibility and reciprocity.* Managing security, hardware and production chains is part of the first area, but it speaks against harshly legislating, and this is followed in the rest as well. Microsoft wanted to indicate that government intervention should be kept at a minimal to keep their corporate influence high. Outside of this moot point, it shows that the debate was an equally prominent level more than ten years ago, and no other research indicates that the threat has lessened since then. Supply Chain Attacks are adversarial attacks on a supply chain. It is well defined because of its critical role and has been discussed in detail in US government reports.[90] However, these are not academic papers, which creates a need for scrutiny of the models proposed. Both suggest a framework to understand the patterns and the structural dangers that these attacks pose, and they do it based on attacks that did

[88] https://nsarchive.gwu.edu/document/22385-document-08-committee-national-security, last accessed 11 December 2024.

[89] Scott Charney and Eric T Werner, *Cyber Supply Chain Risk Management:Toward a Global Vision of Transparency and Trust* (techspace rep, Microsoft 2011) P. 10 - 16.

[90] John F Miller, *Supply Chain Attack Framework and Attack Patterns* (techspace rep, December 2013, MITRE 2013) ⟨https://apps.dtic.mil/sti/pdfs/ADA610495.pdf⟩; Melinda Reed, John F Miller, and Paul Popick, *Supply Chain Attack Patterns : Framework and Catalog* (techspace rep, OFFICE OF THE DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR SYSTEMS ENGINEERING 2014) ⟨https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.648.6043&rep=rep1&type=pdf⟩.

occur, see the appendixes in the reports for patterns. While this is sound, it does not leave room for anything which is not foreseen. The essential assumption for Supply Chain Attacks is that they can occur in all levels of the supply chain.[91] From subcontractor to software or hardware development, to the highest primary party, anyone is a valid target. *Miller* rightfully does not go into the risks which proprietary software or hardware poses, but this still plays a role.[92] Because these tools are not developed by anyone in the supply chain (mostly), but can be attacked regardless of who uses it and who developed it, they must be a separate point to include. Malicious insertions are stated as the primary adversarial attack used against the supply chain, and they will often be multi-staged. This is still very much true, but we now have a range of attacks that do not involve insertions at any point. This could be subversion of control of the CPS, leading to the destruction of goods or injuries.[93] There would be no insertion into the software or hardware, but instead a manipulation of the communication channel to force the CPS to commit to orders not given by the user.

Other authors do divide the attacks into categories. *Eggers* writes that Supply Chain Attacks depend on the area which is targeted. Theft of IP, malicious substitution, alterations, malicious insertion, tampering, and manipulation are just some of the many types than can occur,[94] but they can classically be viewed as falling under the CIA triad. In this case, loss of confidentiality would cover the theft of IP, while loss of integrity would

[91] Miller (n 90) P. 7.

[92] Zach Zhizhong Zhou and Vidyanand Choudhary, "Impact of Competition from Open Source Software on Proprietary Software" (2022) 31(2) Production and Operations Management 731 ⟨https://onlinelibrary.wiley.com/doi/10.1111/poms.13575⟩.

[93] Bonaci and others (n 50). For an overview of an area, see Md Abdullah Al Momin and Md Nazmul Islam, "Teleoperated Surgical Robot Security: Challenges and Solutions" in Xiali Hei (ed), *Advances in Web Technologies and Engineering* (IGI Global 2022) ⟨http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-7323-5.ch009⟩.

[94] Shannon Eggers, "A novel approach for analyzing the nuclear supply chain cyber-attack surface" (2021) 53(3) Nuclear Engineering and Technology 879 (Publisher: Elsevier Ltd) ⟨https://doi.org/10.1016/j.net.2020.08.021⟩, P. 886.

occur during substitution and alterations, and tampering and manipulation would cause real loss of availability. Areas such as nuclear infrastructure which she also handles,[95] clearly require remarkably high degrees of caution.

Following this, I believe we should change the current assumptions concerning Supply Chain Attacks to the following, to include every aspect and generalise it:

1. Supply Chain Attacks can occur anywhere in the supply chain, and to any hardware or software in it, regardless of origin.

2. The attacks can be of any kind.

3. The goal of the attacks must be more than to breach a given system.

What makes this different from a single adversarial attack on one device or system, is that the aim is more than just initiation. The failure achieved on the system is therefore both the loss of for example integrity, but also the following loss of availability through ransomware or loss of confidentiality through privacy failures. We cannot quantify the goals of the attacker under most circumstances because the perpetrators very rarely are identified, but we can derive them from their actions. Prevention or mitigation techniques include anything traditionally used against adversarial attacks, such as organisational measures, encryption, and other classic measures. Of particular interest is mitigation at scale and through simulations and modelling.[96]

[95] Shannon L Eggers, "The nuclear digital I&C system supply chain cyber-attack surface" (2020) 122(June) Transactions of the American Nuclear Society 119.

[96] Kaiyue Zheng and Laura A Albert, "Interdiction models for delaying adversarial attacks against critical information technology infrastructure" (2019) 66(5) Naval Research Logistics (NRL) 411 ⟨https://onlinelibrary.wiley.com/doi/10.1002/nav.21859⟩; Kaiyue Zheng and Laura A Albert, "A Robust Approach for Mitigating Risks in Cyber Supply Chains" (2019) 39(9) Risk Analysis 2076 ⟨https://onlinelibrary.wiley.com/doi/10.1111/risa.13269⟩.

5.5.1 Selected Examples

I will in this section take a closer look at two Supply Chain Attack examples. One targeted all types of sectors, while the other was more focused on commercial targets.

Sunburst Backdoor (SolarWinds Attack)

The first to discover this adversarial failure was the company FireEye, who in their report from 13 December 2020[97] outline what their concerns are.[98] The start of the attack was an update of the Orion IT monitoring and management software. Instead of a valid update, the users downloaded a trojan, and this occurred multiple times between March and May in 2020. What characterizes a trojan is its deceptive nature, with the original reference to the wooden horse used by the Greek Army in the *Aeneid* by Virgil against the Trojans, to leave and hide soldiers inside, describing its purpose precisely. It included legitimate files except for one, the SolarWinds.Orion.Core.BusinessLayer.dll component, a dynamic-linked library file. These cannot be used on their own and must be called up to have any function. This file would then be actively used by the legitimate Solarwinds.BusinessLayer executable file after a two week delay to enable the Sunburst backdoor.

Before making contact back to the adversary, the trojan checks for antivirus and other countermeasures, and a range of information about the machine that it is on. The trojan wants to avoid certain environments that

[97] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html, last accessed 11 December 2024.

[98] A more detailed diagram of adversarial actions with Sunburst can be found here https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html. See also Pratim Datta, "*Hannibal at the gates* : Cyberwarfare & the Solarwinds sunburst hack" [2021] Journal of Information Technology Teaching Cases 204388692199312 ⟨http://journals.sagepub.com/doi/10.1177/2043886921993126⟩.

are inside of SolarWinds Inc., and if it there, it will exit and cease to function after erasing its presence. This shows how specific the attack was, and how much the adversary wanted to avoid detection, but it was identified 7 months after its first entry into a client system by FireEye. The trojan mimics natural SolarWinds API communication, which then enables it to connect to a domain that is controlled by the adversary, a so called command and control domain (C2). The trojan then tries to determine which security software resides on the hardware it is currently placed in, which it does locally and with great efficiency.[99] Even if it finds any of these, it will not exit because of it, instead checking for whether they are active, and whenever they are not, the trojan will disable the security software on the next power cycle in the Windows registry which it creates access to. When the trojan sees that none of the services on the list are active because it has disabled them, it will initiate and let the adversary control it through the C2 domain. This is where the trojan can lead to a range of outcomes, with the most common being Teardrop. Sunburst is known to have dropped other payloads than Teardrop, which by itself is intriguing. Teardrop is purely a means to an end, through an extensive extraction process, including pretending to read information from a picture file, to drop a customized Cobalt Strike Beacon. The latter is modified proprietary software, defined as an asynchronous post-exploitation agent, which is usually used for penetration testing, but in this case has been directly used to attack a system. The beacon enables a massive number of attacks. And with that, the backdoor enables an adversary to do anything within the system. Despite this, there are possible links to existing malware,[100] putting its

[99]For a list of all the types of software it would recognize, which is quite extensive, see https://github.com/fireeye/sunburst_countermeasures/blob/main/fnv1a_xor_hashes.txt, last accessed 11 December 2024.

[100]See https://securelist.com/sunburst-backdoor-kazuar/99981/ last accessed 11 December 2024.

novelty into perspective,[101] regardless of its flawless execution.[102]

Kaseya Ransomware Attack

Unlike the Sunburst Backdoor, this attack was a simpler process.[103] First, the attackers compromised the company Kaseya's Virtual Systems Administrator, with an exploit which was discovered some days prior.[104] The program itself was only used in a limited number of businesses, but most of those that ran it administered other companies' systems at the same time. Because of that, the compromise was exponentially increased by the nature of the service supply chain which the adversaries targeted. The adversaries used this to load ransomware onto a massive amount of businesses, including 800 Swedish Coop stores.[105] This is therefore a case of a digital service supply chain being compromised and used to target physical goods and physical service supply chains, and therefore a good example of a simple but effective Supply Chain Attack.

---

[101] Massimo Marelli, "The SolarWinds hack: Lessons for international humanitarian organizations" (2022) 104(919) International Review of the Red Cross 1267 ⟨https://www.cambridge.org/core/product/identifier/S1816383122000194/type/journal_article⟩.

[102] For additional analysis, see Fabio Massacci, Trent Jaeger, and Sean Peisert, "SolarWinds and the Challenges of Patching: Can We Ever Stop Dancing With the Devil?" (2021) 19(2) IEEE Security & Privacy 14 ⟨https://ieeexplore.ieee.org/document/9382358/⟩ accessed 2 September 2023; Lavi Lazarovitz, "Deconstructing the SolarWinds breach" (2021) 2021(6) Computer Fraud & Security 17 ⟨http://www.magonlinelibrary.com/doi/10.1016/S1361-3723%2821%2900065-8⟩ accessed 2 September 2023; Sean Peisert and others, "Perspectives on the SolarWinds Incident" (2021) 19(2) IEEE Security and Privacy 7; Jeferson Martínez and Javier M Durán, "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study" (2021) 11(5) International Journal of Safety and Security Engineering 537 ⟨https://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.110505⟩; Pratim Datta, "*Hannibal at the gates* : Cyberwarfare & the Solarwinds sunburst hack" (2022) 12(2) Journal of Information Technology Teaching Cases 115 ⟨http://journals.sagepub.com/doi/10.1177/2043886921993126⟩ accessed 2 September 2023.

[103] https://www.riskbasedsecurity.com/2021/07/12/the-kaseya-attack-everything-to-know/, last accessed 11 December 2024.

[104] https://csirt.divd.nl/2021/07/04/Kaseya-Case-Update-2/, last accessed 11 December 2024.

[105] https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant, last accessed 11 December 2024.

5.5.2 Cyberphysical systems and IoT

To finish the technical Supply Chain Security part of this chapter, I include some commentary on CPS and IoT in the context of supply chains in general.

Physical and even digital supply chains have evolved since 2011.[106] But CPS and IoT have dominated the world, especially the world of supply chains. In turn, this also affects which consequences Supply Chain Attacks can have on its targets. CPS refer to systems that have network access and which seamlessly integrate computation and physical components into operation,[107] and which usually have more than two levels, with sensors on the bottom, a network for these, and a top which controls the entire system.[108] On the other side of this, we have the increased use of IoT, which act as network connected sensors that may part of a CPS or greater systems.[109]

The key between each is the network access, a means to integrate a computer into anything, anywhere. An attack with simplicity of the one done on Kaseya can at any point knock out payment systems or physical stores, ticket dispensers or anything else that is loosely connected to a service supply chain above it. These two types of technology therefore make supply chains much more vulnerable to adversarial attacks than ever before.

Security and Safety Constraints

Increased use of systems of systems like CPS may therefore decrease safety and potentially security. The first is due to all the ways these systems can fail. Any modern production facility will likely make use of CPS

[106] Charney and Werner (n 89).
[107] NSF (n 24).
[108] Kobara (n 40).
[109] Xenofontos and others (n 168).

and IoT at once.[110] This means that any attack on the main control systems will be able to shut down lower levels of the plant with ease, which in turn can cause a failure, either halting production or harming the employees. The same use of these systems decrease security overall, because the amount of entry points increase incrementally with the added features of IoT devices, each being an new door for adversaries.[111] We can extrapolate this to Supply Chain Attacks, as the same kind of failures caused by a single attack to shut down production, may be used to affect and constitute an actual Supply Chain Attack at the same time. IoT has a further issue, which is planned obsolescence. Unless produced and serviced by its users, IoT products have short lifespans,[112] and after this they are to be considered significant security threats. If they are then a part of a greater digital supply chain, they potentially risk losing confidentiality, integrity, or availability of the entire system.

The next section dives into the implementation of NIS1 in three national legal systems, and other perspectives as to how they can prevent Supply Chain Attacks.

[110]H D Nguyen and others, "Industrial Internet of Things, Big Data, and Artificial Intelligence in the Smart Factory: a survey and perspective" [2019] 6; Glenn Tucker, "Sustainable Product Lifecycle Management, Industrial Big Data, and Internet of Things Sensing Networks in Cyber-Physical System-based Smart Factories" (2021) 6(1) Journal of Self-Governance and Management Economics 9 ⟨https://addletonacademicpublishers.com/contents-jsme/2091-volume-9-1-2021/3944-sustainable-product-lifecycle-management-industrial-big-data-and-internet-of-things-sensing-networks-in-cyber-physical-system-based-smart-factories⟩; Javier de las Morenas and others, "Security Experiences in IoT based applications for Building and Factory Automation" (IEEE February 2020) ⟨https://ieeexplore.ieee.org/document/9067229/⟩.

[111]Elizabeth LaGreca and Chutima Boonthum-Denecke, "Survey on the Insecurity of the Internet of Things" (2017); Sihan Wang and others, "Insecurity of operational cellular IoT service: new vulnerabilities, attacks, and countermeasures" (ACM October 2021) ⟨https://dl.acm.org/doi/10.1145/3447993.3483239⟩.

[112]Narges Yousefnezhad, Avleen Malhi, and Kary Främling, "Security in product lifecycle of IoT devices: A survey" (2020) 171 Journal of Network and Computer Applications 102779 ⟨https://linkinghub.elsevier.com/retrieve/pii/S1084804520302538⟩.

5.5.3 National Law

Unlike the overarching guidance and general rules of the EU, national law applies and functions directly onto the supply chains and its links. I here look at three different legal systems and focus on how they each handle the NIS1 implementation[113] and Supply Chain Security.[114] The latter is not speculative, but a matter of showing the existing ways which security guidance or rules can be enforced, and considerations on expropriation or similar harsh legal actions, even if the measures seem extreme or are close to impossible.

Manufacturers are legal entities, and each national state has rules to punish or otherwise force legal entities to comply. Furthermore, national states can always act as private partners, and create contracts and arbitration systems that can further convince manufacturers and other parties to mitigate as many Supply Chain Attacks as possible. We therefore might not need to look to the future for means and tools that can be used to increase security and safety for everyone. Conversely, there are emerging consequences from not applying national law to global private entities in this area.[115]

All three countries share two measures that they can each implement directly. First, contractually binding providers of security and other supply chain parties, private to private party. Second, creating binding legal obligations for the supply chain at large, either specific security links or the main responsible parties, or any combination of this. States can and are naturally contract partners,[116] and it is through this that they would be

[113] NIS2 will be briefly discussed in 6.5.6.

[114] Users are worth studying too, see, e.g., Nisreen Ameen and others, "Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce" (2021) 114 Computers in Human Behavior 106531 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0747563220302831⟩.

[115] Ido Kilovaty, "Privatized Cybersecurity Law" (2019) 10(4) Irvine Law Review.

[116] Jukka Ruohonen, "An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union" (2020) 5(2) European Journal for Security Research

able to bind and force mitigation of Supply Chain Attacks. The issue with doing so, is effectiveness and willingness of the participants. Any link of any major supply chain, or a security provider, has no interest in legally binding itself to terms without something in return, and solving issues in courts will as always be lengthy and costly. Arbitration clauses would be a possibility with such agreements, but since the state would act as a private party under those circumstances, any other actor could simply refuse to sign the contract in the first place.

However, any measure from the state to force links of a supply chain to sign the contract, would change the state from a private party to a public party, because of its violation of the principle of contractual loyalty and abuse of powers. This would distort the relationship, removing the private legal aspects entirely or partially.

The contract solution would be widely different between the UK, Ireland, and Denmark respectively, due to the various roles of background law.[117]

Creating new legal obligations is not novel, but currently none of our examples have direct legally binding obligations for the mitigation of Supply Chain Attacks. Any state, including our three examples, have the means to create these and enforce them as well, even if most supply chains are global or at least regional. Despite these measures existing, national states still have the power over individual workers or the physical infrastructure, therefore eliminating any arguments against the futility of the action.

349 ⟨http://link.springer.com/10.1007/s41125-019-00053-w⟩.

[117] Like case law on how contracts are viewed in Common Law versus how they are viewed in Scandinavian law where contract legislation plays a bigger role, although the latter now exists everywhere.

Denmark

Implementation The NIS1 directive is implemented in Denmark via a range of laws and binding guidance.[118] I will take a closer look at those that relate digital supply chains, but it is worth noting that there are strict direct requirements to levels of security for all 7 points mentioned in Annex II in NIS1, and each has its own binding guidance that the area *must* follow or face fines.[119] The main implementation law defines essential services the same way as the Directive, but outside of essential financial service providers,[120] the exact list is secret or implied. § 4 is however the security specification, in that providers of essential services must control known risks, have adequate security compared to the risks and mitigate or prevent adversarial events from occurring to their systems.[121]

Each different piece of guidance derived from the main implementation text may have different authorities being responsible. Fines are loosely defined and far lower than those in the other two examples, and this is due to a different culture regarding trust and a much tighter grip on public essential services.[122] The latter enable changes and internal punishments for individuals based on labour law, not considered in the implementation, and restructuring or changes that could increase security without it being

[118]The main implementation act can be found here: https://www.retsinformation.dk/eli/lta/2018/436, last accessed 11 December 2024. The rest can be found under "Yderligere dokumenter", then "Se detaljeret overblik".

[119]See for example security guidance for the electricity and gas providers, https://www.retsinformation.dk/eli/lta/2021/2647, last accessed 11 December 2024.

[120]https://www.finanstilsynet.dk/tilsyn/information-om-udvalgte-tilsynsomraader/it-tilsyn/udpegelse_af_operatoerer_af_vaesentlige_tjenester, last accessed 11 December 2024.

[121]For perspectives outside of law, see Sergei Boeke, "National cyber crisis management: Different European approaches" (2018) 31(3) Governance 449 ⟨https://onlinelibrary.wiley.com/doi/10.1111/gove.12309⟩.

[122]There is little research in English on this exact topic, but see Øystein Pedersen Dahlen and Helge Skirbekk, "How trust was maintained in Scandinavia through the first crisis of modernity" (2021) 26(1) Corporate Communications: An International Journal 23; Frank AG Den Butter and Robert HJ Mosch, "Trade, Trust and Transaction Costs" (2003) 3 TI Discussion Paper; Cornelius Cappelen and Stefan Dahlberg, "The Law of Jante and generalized trust" (2018) 61(4) Acta Sociologica 419.

public or regulated tightly by the implementation law.

Other Measures The law of stock and partial companies in Danish law[123] enables the Danish Business Authority to forcefully close the most common types of companies in the country.[124] The first two categories could theoretically be used for the failure to mitigate Supply Chain Attacks, but it is very unlikely, as forceful closure is usually related to rules of process or violation of minority shareholder or creditor rights. But, working against the purpose of the company as well as the "wrong" leadership are legitimate reasons, which is why it must be mentioned.

The other direct means which the Danish state has, is the expropriation of the company or the entire Supply Chain. This can theoretically be done through the Danish Constitution,[125] but has never been done in this way before. In a given situation where it would be necessary, such as during a national crisis, a freer and less restraining measure could be used instead, like contractual obligation or emergency obligations issued via law.[126]

United Kingdom

Implementation Even if the UK is an EU-member no longer, it implemented the NIS1 directive when it entered into force.[127] It did so through different means than Denmark. The legal implementation is done through the Network and Information Systems Regulations 2018[128] which desig-

[123]Law nr. 763 of 23 July 2019, https://www.retsinformation.dk/eli/lta/2019/763, last accessed 11 December 2024.

[124]See § 225, part one.

[125]§ 73, part one, requires expanded view of "property", which is acceptable since ownership of shares etc. is considered "property" of the individual, and companies are considered legal individuals owned and run by citizens.

[126]This was seen on a widespread level during the Covid-19 pandemic, but this has so far not been regarding security and safety of supply chains.

[127]For other perspectives, see Madeline Carr and Leonie Maria Tanczer, "UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions" (2018) 3(3) Journal of Cyber Policy 430.

[128]Statute No. 506, 2018.

nates competent authorities as those that can enforce the rules and defines which types of penalties that are supposed to encourage compliance. Furthermore, the UK implemented a series of thorough guidance and systems, such as the Cyber Assessment Framework. The relevant authority, which depend on the area of essential services, has quite the range of powers, including right to retrieve information or inspect,[129] and the penalties are fines.[130] What is very intriguing are the grounds for the fines, which is either non-compliance through notices or not following orders, or not reporting incidents in various ways.[131] Like Denmark, there seems to be no expansion of the concept of critical infrastructure to include cybersecurity providers at large.

Other Measures The UK can intervene and forcefully close companies and other legal entities. Unlike Denmark, the rules regarding this are tightly defined and leave little room for cases where security or mitigation of Supply Chain Attacks could be the basis of it. If the company is clearly defunct, which in some situations where destitute software is used may be the case, the company can be stricken off within 2 months.[132]
There is a theoretical possibility for something else in the Insolvency Act 1986, section 124 A. This section allows for winding up on grounds of public interest, which could include failure to comply with security requirements to prevent Supply Chain Attacks in the future. At present, the closest we get is closure due to fraud investigations, section 124 A, c, but because of how the section is shaped, it would be possible to add further reasons for winding up that could function as deterrence and reasons to comply. The case law concerning the statute allows for closures within

[129] See Part 5, 15.
[130] See 18(6).
[131] See 17(10).
[132] See the Companies Act 2006, 1000(3), assuming no answer is given from the company in question.

even more subjective terms.[133]

Expanding the idea of expropriation in UK law to include punishments for damaging supply chains is difficult. Since there is no written constitution,[134] we must rely on statutory law,[135] which is too specific and not reliant on case law to contain rights for the state that could include situations where a company and its assets must be acquired to mitigate Supply Chain Attacks. In terms of the other solutions and measures, the UK is therefore quite limited.

Ireland

Implementation Initially, Ireland has implemented the NIS1 directive through a Statutory Instrument like the UK, No. 360 of 2018, but its content and structure is quite different. As is the lack of deliberately abstract guidance which, like Denmark, does not exist. Definitions of operators of essential services and what is otherwise needed are here, but one noticeable difference is clear, as fines and investigations are done through either designated authorities[136] or authorized officers.[137] The latter is interesting but does not mean there will be differences in enforcement, which is found in regulation 34. Like the other two jurisdictions, fines are the chosen tool, and they too have not expanded their concepts to include security providers at large.

Other Measures Rights and obligations of Companies and related authorities are regulated in the Companies Act 2014. Companies can be

[133] See, e.g., *Re Alpha Club (UK) Ltd (2002)*, para 19.

[134] See, e.g., The Rt Hon Lord Scarman, "Human Rights in an Unwritten Constitution" (2012) 2(1) The Denning Law Journal 129 ⟨http://www.ubplj.org/index.php/dlj/article/view/163⟩; Justin O Frosini, "Is Brexit Ripping up the Unwritten Constitution of the United Kingdom?" (2019) 11(1) Italian Journal of Public Law.

[135] Such as the Planning and Compulsory Purchase Act 2004.

[136] Statutory Instrument No. 360 of 2018, regulation(reg.) 7 and 8.

[137] Reg. 28.

stricken off the register by the Registrar,[138] in our case if they fulfil the requirements set out in section 726. However, none of these requirements can include violation of security or other obligations related to Supply Chain Attacks, which like with the UK, leaves this method of compliance out.

Expropriation in Irish law is derived initially from the Constitution, specifically Article 43(2)(2). Like the Danish constitution, the Common Good is the pivotal point, as is "occasion requires". The latter refers to when the State can expropriate private property, which is the core protection of Article 43 outright. Land Laws[139] implement those powers for relevant situations, but like Denmark, there is theoretical room for potential expropriation of companies.

5.5.4 The Application of the CRA on Supply Chain Security

The CRA represents a huge step forward for the regulation of cybersecurity. If its purpose is read to include individual parts of Supply Chain Security, it will also have a lasting impact on this field as well. Normally, Supply Chains are heavily privately regulated, with consequences from malpractice, including in security, only creating consequences for the parties involved in litigation. The exception to this could be NIS1 or NIS2 based interruptions by EU Member States.[140] The CRA reverses this and requires that the manufacturers of all types of cybersecurity supply chain links much reach CE certification and comply with additional standards, to be allowed to be used and sold in the EU. Everyday parts of supply chains,

[138]Companies Act 2014, section 725.

[139]See, e.g., the Land and Conveyancing Law Reform Act 2009.

[140]I will answer shortly on how NIS2 may change the situation presented above in the following subsection.

such as the OS on a server, the smartphones of employees, the computer used by security staff in a harbour; all of these and many more will be subject to minimal cybersecurity requirements, which many did not have to adhere to before. We can assume this will increase security for all types of supply chains at large, even if only the bare minimum criteria are fulfilled, gaining a net positive effect outside of the damage it may cause to free and open source software,[141] and other actors who cannot for logistical or resource reasons implement the CRA.

Applying the CRA will therefore be decentralised, and not on the supply chains as such, which represents oversights in cybersecurity sense. Viewing and understanding the Supply Chain Security of the entire supply chain will not be regulated or done via the CRA, meaning that this area is still not directly regulated, and cannot help to solve the issues present in the new framework in section 5.5. The Cybersecurity Act in the EU, and national cybersecurity legislation may be relevant here, but only in the way I have suggested above.

5.5.5 NIS2 Directive Considerations

NIS2 improves many areas of the NIS1 directive but does not diverge significantly from it.[142] The main criticisms from the NIS1 implementation was the fragmented and very varied way which Member States understood

[141] Many organisations have reacted, see the open letter from Open Source Matters, WordPress Project, TYPO3 Association and Drupal Association, representing 50 percent of all FOSS activity in the EU, https://www.joomla.org/announcements/general-news/5891-open-letter-foss-cms-cyber-resilience-act.html, last accessed 11 December 2024.

[142] See early papers such as Philipp Eckhardt and Anastasia Kotovskaia, "The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive" [2023] International Cybersecurity Law Review; Sandra Schmitz-Berndt and Pier Giorgio Chiara, "One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive" (2022) 3(2) International Cybersecurity Law Review 289 ⟨https://link.springer.com/10.1365/s43439-022-00058-7⟩ accessed 2 September 2023.

and incorporated the rules and the spirit into their jurisdictions.[143] As can be seen from the analysis above, even with a few examples, there are quite different administrative solutions to it as well, which NIS2 will hopefully change and streamline. This is to be done with more narrow ways to implement the directive[144] and clearer definitions,[145] including on Supply Chain Security considerations specifically for the Member States.[146] Secondarily, the mandated (as much as possible) use of Cyber Response Incident Teams will consider Supply Chain Security and Attacks closely.[147] Thirdly, the newly established Cooperation Group will also focus strongly on coordination for preventing and handling Supply Chain Attacks, which may have a further positive effect on the Supply Chain Security in the EU. This paints an optimistic, and even positive picture with regards to Supply Chain Security, except that we can only know when it is fully implemented, and then understood in the context of each Member State.
Additionally, due to the cumulative application of both NIS2, the CRA, and all the other cybersecurity legislation I looked at in section 5.2.1, Supply Chain Attacks earlier may be adequately considered, though notably, the private actors who make up a majority of the chain are not involved or considered in NIS2.

5.5.6 Regulating Adversarial Supply Chain Attacks in the Future

In this section, I go through two potential future scenarios that may or may not justify the increased focus on mitigating Supply Chain Attacks, as well as some general thoughts on future legal mitigation approaches. The two

[143] Schmitz-Berndt and Schiffner (n 18).
[144] See especially NIS2 Directive, Art 5, with its minimum requirements.
[145] See Art 7, 8, 9 for general Member State obligations, and Art 20 and 21.
[146] Art 21(3).
[147] Art 14(4)(i), and in Art 22.

are shipping systems and the chip supply.

Leveson, Nancy G. once commented on a crucial assertion regarding the use of computers in general:[148]

"There is no technological imperative that says that we must use computers to control hazardous functions."

Increased uptake of technology that is vulnerable to certain types of adversarial attacks will result in increased successful attacks. However, this kind of argumentation is pointless because it does not attempt to *ex ante* predict and/or mitigate the failures. We know that increased automation may not always result in increased productivity, and that it may decrease safety of the system, and from what he has discussed earlier, it is also clear that it will decrease security. But security can be improved, and this is where the discussion becomes more concrete.

To show this, I look at a type of Supply Chain Attack that may become prevalent in the future, and which has worldwide consequences.

Shipping goods is facilitated with greatest profit and lowest cost per ton possible in mind.[149] If this can further be reduced, through automation and use of increased IoT, it is likely that the companies will make use of it. Furthermore, all ships of this calibre are tracked by the Automatic Identification System on a global scale, make use of GPS, make use of radars and if automated, would make use of a vast number of new sensors and potentially robots, with no or few humans on deck. All these subsystems/"subcontractors" can be compromised, either individually or from the control systems suffering failures. The latter could be on the ship, or in the headquarters if they have a constant connection. And as we saw with the Sunburst Backdoor, the security provider which is used could be com-

[148] Leveson (n 163) P. 405.

[149] SR Tolofari, KJ Button, and DE Pitfield, "Shipping Costs and the Controversy Over Open Registry" (1986) 34(4) The Journal of Industrial Economics 409 ⟨https://www.jstor.org/stable/2098626?origin=crossref⟩.

promised as well. As of the time of writing, there are measures in place to mitigate automation failures, as ships can be sailed without any of these systems. But in the future, this may not be the case, and the entire infrastructure of the whole world may be at risk from Supply Chain Attacks,[150] and past incidents further support this.[151]

However, there is an even more pressing, though not unknown type of attack that can hit the very origin of CPS or IoT. Semiconductors, used to make processing and other power for the very devices that can be attacked, can be equally hit by Supply Chain Attacks.[152] Because there are extremely few main providers of these, the entire supply of the very basics of our digital infrastructure can be shut down in a matter of days. And while these attacks can hit the system of manufacturing or distribution, the chips and other devices themselves can be attacked directly at the plant where they are produced, potentially compromising any computer or device they are part of.[153] Together with striking the supply chains through every type of system imaginable, the entire world economy is potentially at risk from Supply Chain Attacks in the future.

5.5.7 Future Regulatory Mitigation Techniques

As I showed earlier, national jurisdictions do not always have many choices to prevent or otherwise regulate Supply Chain Attacks considering the

[150] Boris Svilicic and others, "Paperless ship navigation: cyber security weaknesses" (2020) 13(3-4) Journal of Transportation Security 203 ⟨https://link.springer.com/10.1007/s12198-020-00222-2⟩.

[151] Per HÁkon Meland and others, "A Retrospective Analysis of Maritime Cyber Security Incidents" (2021) 15(3) TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation 519 ⟨http://www.transnav.eu/Article_A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents_Meland,59,1144.html⟩.

[152] Jeffrey Voas, Nir Kshetri, and Joanna F DeFranco, "Scarcity and Global Insecurity: The Semiconductor Shortage" (2021) 23(5) IT Professional 78 ⟨https://ieeexplore.ieee.org/document/9568259/⟩.

[153] Chen Dong and others, "Hardware Trojans in Chips: A Survey for Detection and Prevention" (2020) 20(18) Sensors 5165 ⟨https://www.mdpi.com/1424-8220/20/18/5165⟩.

potential consequences they can have. This will change with the implementation of NIS2 (though not in UK Law), with the literal mentions of Supply Chain Security. However, extreme national legal measures will rarely be used, and in a European context, regulation from the European Union is the best bet at horizontal hard legal rules to mitigate devastating attacks. From an international perspective, examples such as Executive Order (E.O.) 14017 on America's Supply Chains[154] or requirements set by state purchasers worldwide, like a Software Bill of Materials in the US,[155] represent immediate action, but do not contribute to a clear legal landscape or further technology specific requirements.

Otherwise, fines and very theoretical approaches to expropriation and emergency measures[156] are not enough to fully and truly mitigate the attacks going forward. Technological developments are ongoing, but this does not mean that we need to throw out the champagne with the cork. Existing enforcement measures in other areas can be reused, but a range of newer and more experimental enforcement measures could be considered, like financial incentives, tax breaks[157] or direct ministerial or public oversight. From this, the choice of merely fining the providers and not employing stricter punishments in the form of threats of forceful closure or punitive punishments for directors or other responsible officers seems unwise if deterrence is the only tool available,[158] akin to the criminal liability which

[154]Jake Sullivan and Brian Deese, *Executive Order on America's Supply Chains: A Year of Action and Progresss* (techspace rep, White House 2022) ⟨https://www.whitehouse.gov/wp-content/uploads/2022/02/Capstone-Report-Biden.pdf⟩.

[155]Carmody and others (n 65).

[156]During a state of emergency, many states can employ special written or unwritten rules beyond what is mentioned here, but these are so rarely seen and unclear, that I have not included them.

[157]There is a greater discussion on whether these or financial incentives have their intended effect as well.

[158]If moral responsibility and corporate guilt could be implemented, this may provide more efficient means to compliance, Heli Korkka-Knuts, "Behaviourally informed approach to corporate criminal law: Ethicality as efficiency" (2022) 10(1) Bergen Journal of Criminal Law & Criminal Justice 30 ⟨https://boap.uib.no/index.php/BJCLCJ/article/view/3689⟩. This is because criminal punishments in corporate settings has its own is-

exists for companies which handle explosives or chemicals in many jurisdictions.[159]

5.6 Conclusion

In this chapter, cybersecurity legislation in the EU has been analysed, specifically the proposed CRA and the established NIS1 directive. I showed how they have been applied in practice, and their application and understanding were viewed through the notion of Supply Chain Security and Attacks.

Resilience is achieved from both applying defences, mitigation techniques, and recovery mechanism for when the first two fail; the CRA and especially NIS2, when implemented, will provide this. The CRA presents broad a product-based approach to cybersecurity regulation, and while independent, will in this manner work together with existing legislation to fulfil its role within the broader net of regulation. Sadly, the CRA is product legislation, meaning that it does not have the Member States themselves as a primary subject, nor supply chains, and its compliance and enforcement mechanisms will therefore proportionally suffer. But it brings hope and minimal cybersecurity requirements, which should improve cybersecurity both in the EU and outside of it due to the Brussels effect.

The second aspect of this chapter is its contribution to understanding Supply Chain Attacks better in the context of its regulation and its nature, which was done by broadening existing definitions deliberately, showcasing two examples of such attacks, and analysing existing NIS1 implemen-

sues,Robert Luskin, "'Caring about Corporate 'Due Care': Why Criminal Respondeat Superior Liability Outreaches Its Justification" (2020) 57(2) American Criminal Law Review 29.

[159]W Allen Spurgeon and Terence P Fagan, "Criminal Liability for Life-Endangering Corporate Conduct" (1981) 72(2) Journal of Criminal Law and Criminology 35.

tation in three jurisdictions. By realising that any kind of adversarial attack, in any part of the chain, can lead to Supply Chain Security failures, a greater and more all-encompassing way to understand the term is gained, which reflects reality. This includes acknowledging that Supply Chain Attacks must do more than merely breach a link in the chain but must escalate or otherwise enable the adversary to take further action.[160]

Moving to some general conclusions, I should answer the questions posed in the introduction[161] as they relate to Supply Chain Security.

Horizontal requirements for almost all types of products as a legal concept is large, and combined with supply chain legislation, makes for a contrast when put into a cybersecurity context. Resilience as a legal term is well known, since deployment of cybersecurity, per good practice and legislation, should include means for systems to fail in ways that do not impact others or interconnected systems. Security views these three concepts as technical hurdles and compliance problems, but also acknowledges the complexity they can be. The chapter clearly showed concrete examples in both legislation and cases, and it only touches the surface of how complicated it is. The complexity stems from many smaller subsystems being connected to others, and they themselves affecting both individuals and companies - all of which makes for exponential increases in complexity. Resilience, if built in, is viewed as a welcome additions in security, but if done poorly, can be seen more as a mere compliance exercise, and something which, due to costs, will be difficult being realised in practice. Supply Chain Security as a legal concept is welcomed, as it will create more secure systems, but doubtlessly also an increase in complexity when designing, building, and deploying them.

[160] Otherwise, it is just a singular adversarial attack causing a security failure.

[161] "How can this legal concept be understood in cybersecurity", and "how can these cybersecurity considerations be understood in law"?

Resilience and Supply Chain Cybersecurity, as viewed by law, play out quite differently. They represent vast increases in complexity that cannot be easily handled by public legal rules, conventions, Private Law, or anything in-between. Resilience taps into existing product regulatory ideas, but can be wildly complicated to manifest, and the increased costs and complexity will disincentivise companies, and even states, from actually fulfilling them. As noted earlier in the thesis, security is not the same as having waterproof systems, meaning that resilience should be a natural aspect of the security of most systems, giving a reason why legislation like the CRA is necessary. Having law acknowledging the need for boundaries, and setting up frameworks is what things like the GDPR was very successful in doing, and there is no reason not to continue this trend here. Supply Chain Cybersecurity can be viewed in this light too, as law both now, and for an extended period depending on jurisdiction or through an international law lens, has recognised the need to attempt to control, or at least increase security in critical infrastructure and throughout essential supply chains, whether private or public. NIS2 is the strongest attempt yet at this, but this leaves the cross-border and international links untouched, due to their contractual and subsidiary-based nature. The thesis cannot answer the latter, but it clearly is a way that law also views resilience and supply chain security.

6 | Conclusion

Law and cybersecurity are from different academic realms, but this thesis has illustrated that they have many things in common.

This was despite its limitations, which consist of lacking empirical legal and cybersecurity-related work as to the behaviour of manufacturers, and lacking a fully developed new interdisciplinary methodology, instead relying on multidisciplinary and partially interdisciplinary approaches to the questions posed and the analysis. This limits the thesis in what it can contribute to; while it has provided the legal and cybersecurity communities with published research, the thesis is not the end point in terms of combining law and cybersecurity. It provides a starting point but does not comprehensively showcase every single interaction, but this is accounted for by its initial limitation as analysis in the introduction.

The thesis consisted of the following chapters:

- A necessary introduction in Chapter 1.
- Chapter 2 illustrated the background and methods of the thesis, for both law and cybersecurity respectively, and an overview of the applied methods in each chapter.
- In Chapter 3, medical devices were the focus; analysis of the EU legislation surrounding them in detail, how surgical robots are to be understood, how adversarial attacks on these function, how the

notion of intention works in practice in this legislation, and how adversarial attacks interact with Private Law in Danish Law.

- Chapter 4 examined Client-side Scanning, with an example of it in practice, how it is understood, how it interacts with the European Convention on Human Rights, with analysis of specific relevant rights, and how upcoming legislation will use it.

- Chapter 5 discussed resilience, the proposed Cyber Resilience Act in the EU, and the case of Supply Chain Attacks, based on the implementation of the Network and Information Security Directive in the EU in three jurisdictions, with additional considerations as to how the area can be regulated in the future.

The main findings are as follows:

Chapter 3 showed that definitions and circumvention can play a huge role in law, causing it to *not* affect cybersecurity. This is seen with the requirements put onto cybersecurity not existing if the regulated software and/or hardware is outside the definitions of a given piece of legislation, here the Medical Device Regulation in the EU, a classic problem which can be solved by interpreting such texts more narrowly. However, the consequences of not doing so will be in violation of the purpose of the Regulation. Secondarily, Chapter 3 also illustrated concrete requirements for cybersecurity, in this case for surgical robots. A novel theoretical engineering framework is developed, which combines cyberphysical systems theory with surgical robotics to illustrate the specific adversarial failures surgical robots can suffer. Chapter 3 then illustrated how courts, with Danish law as a case study, may not need to change their evidential processes to accommodate cybersecurity, such as issues with third parties causing damage with cyberattacks. Finally, it offers a technology-neutral means to

solve disputes arising from adversarial attacks in the form of the Danish system of Patient Reimbursement.

In Chapter 4, Human Rights Law shines a light on contemporary surveillance issues, such as Client-side Scanning, regarding pictures on smartphones and other devices. Firstly, a novel definition of Client-side Scanning attacks is developed, then security analysis on these types of systems is presented, and a specific type of Client-side Scanning is discussed. Secondly, through case law analysis from the European Court of Human Rights, vulnerabilities regarding admissibility and protection of property will adversely affect trials if proof from the Client-side Scanning-based methods used is shown, especially on devices such as smartphones due to their personal nature. Finally, it connects these observations with two upcoming pieces of legislation in the UK and the EU.

Chapter 5 delved into the concept of resilience, which must encompass everything before and after a security failure occurs and, accompanying this is a short analysis of the Cyber Resilience Act proposal showing its structure and primary regulatory mechanisms for security. As with all product legislation in the EU, the Act will rely on the practice of authorities and the willingness of companies to comply with it, while regulating the integral area of cybersecurity, and will be applied to Supply Chains. In addition, the reality of the cybersecurity of supply chains is the other focus of Chapter 5, and it concludes that strong legislation is needed on the background of a comparative legal study, and on a case study of Supply Chain Attacks that have occurred. This is due to the profound impact that any successful attack can have, and how many entry points exist in any type of supply chain, be it service, physical goods, or digital. Furthermore, the consequences of any successful adversarial failure on any worldwide supply chain are far too great for contracts and other non-statute means of

regulation. However, newer legislation in the area does provide hope.

The thesis shows that law and cybersecurity mutually influence each other and do so in unique ways that are part of the greater complex of law and technology as a field. They did so while retaining unique characteristics because of the methods and reasoning which they share, and because cybersecurity has received roles in the world which physical security used to maintain.

6.1 Future Steps

The chapters each indicate questions which need to be answered in future work. This section summarises these.

Software, robots, and cyberphysical systems such as medical devices represent a great clash between safety and cybersecurity, as security failures can cause physical injuries. Law shapes cybersecurity because it poses compelling requirements for the level of security necessary, and because it sets standards and principles that developers are supposed to follow. This thesis explores means to include and enforce EU law to prevent or mitigate adversarial attacks in medical devices, which then leaves the question of enforcement, the necessity of more empirical research into how each national authority enforces its rules, and additional research into accessories for medical devices. Accessories create boundary problems in the form of questions on liability and behaviour between manufacturers and developers, and showcase issues with overlap, especially regarding software, both in the context of medical devices but also in other product legislation.

To answer the questions which bringing adversarial attacks directly into law pose, further research on how adversarial attacks and defects in cyberphysical systems affect national and international law should be con-

ducted.

Instead of leaving it to concepts in critical infrastructure, Laws of War, or Data Protection, attacks and defences in cybersecurity must become their own legal domain.[1] This must be done to uncover whether cybersecurity can be regulated by modernised mechanisms from older security legislation, instead of being legally controlled in the fragmented manner represented in this thesis.[2] From a Private Law perspective, further research is needed into how product liability, broadly speaking internationally, views defects caused by adversarial attacks.

Law shapes surveillance, another large area which has cybersecurity as one of its main anchors. Wide-reaching and sweeping surveillance concepts, such as Client-side Scanning, must be thoroughly inspected before and during their deployment, as they are quite different from those covered in existing research due to their scale and autonomy. This is future work for the field, but it should also be considered good practice and customary. The human, legal, and economic costs of Client-side Scanning should be explored in further detail, as well as the proportionality of even using such approaches. The latter may seem like a political decision, but as shown in this thesis, it can be achieved based on case law as well, making such limits and thoughts on deployment further grounded in what is and was acceptable in the past in a Human Rights Law context.

Cybersecurity, in turn, also shapes law because of its ongoing change and development, as with the advent of IoT and the increased use of digital systems. The role and development of the draft CRA and similar legislation is a good example of this. Law must focus on how cybersecurity

[1] This has happened with various concepts from the EU, such as the Cybersecurity Act, the draft Cyber Resilience Act and both NIS1 and NIS2. However, none focus entirely on cybersecurity, instead they are either internal EU law, product regulation, or directives for countries, respectively.

[2] This could also further improve the field which cybersecurity stems from, security, see Leveson (n 163).

is deployed and overseen in practice and must include safety perspectives because of the potential consequences which security failures can have. Research in both law and cybersecurity, or within a multidisciplinary or interdisciplinary framework, should explore these clues further, and ongoing reviews of the CRA and its application in practice.

This thesis also focused on how the technical reality of supply chains of all kinds must require the law to follow suit in protecting this complicated infrastructure. Legal analysis of the regulation of supply chains and critical infrastructure, and the exploration of organisational or other means to make supply chains more secure, should be further analysed academically. Secondly, new liability schemes or other means to make existing and future enforcement a reality must be researched further. This is because current cybersecurity legislation is too easy to comply with, in the form of the fulfilment of standards and more, without any inspection or repercussion mechanisms for when the systems stop complying.

6.2 Final Remarks

First, we must review whether the thesis was able to answer the two questions in the introduction, which were "How can this legal concept be understood in cybersecurity", and "How can these cybersecurity considerations be understood in law"?

This thesis was able to answer the two questions posed in three different ways. These can each be found at the end of Chapters 3, 4, and 5. In Chapter 3, the answer to the first question was the new twofold nature of medical devices. Firstly, it represents means to increase security, due to its consequences if the devices fail from adversarial attacks, but also has a new compliance nature for security practitioners. For the second question,

the chapter notes that cybersecurity in medical devices in law is very intimate, necessary, and product regulation, but with special elements which come with working in the medical world. In Chapter 4, the first question is answered by observing the protective nature of Human Rights Law and cybersecurity, and its necessary compliance-like elements. Question two is examined with CSS being a surveillance measure, and being justified through its technical implementation, which if not fulfilled, can speak directly against its existence, especially considering the complexity of allowing it within national law when considering ECHR case law. Finally, in Chapter 5, the first question can be answered succinctly with "complexity", as security views this type of compliance, in the form of resilience, as complicated problems which must be answered both legally and technically. In the second question, the law views supply chain security as necessary, but difficult to implement in practice due to it always existing across borders.

This thesis, in this way, explored answers to these two questions in three different domains, and the two questions illustrated how the thesis fulfilled its purpose of exploring the interaction between cybersecurity and law.

Law and cybersecurity fit and synergise well together, both methodologically and in practice. This thesis has analysed this and explored how this might be achieved within different contexts. It also conveyed hope for both the increased level of cybersecurity, to the benefit and security of all, and hope in the creation of legislation which understands and considers cybersecurity. Not only does this benefit regulatory mechanisms, but it also ensures the safety and security of those affected by digital systems. Current cybersecurity and the law must learn from prior security, safety, and legal research into how technology is regulated. Increased requirements for cybersecurity should be directly proportional to the necessary legal re-

quirements and enforcement to make sure that the systems are safe and secure going forward.

Bibliography

Abelson H and others, “Bugs in our Pockets: The Risks of Client-Side Scanning” (_eprint: 2110.07450, 2021) ⟨http://arxiv.org/abs/2110.07450⟩.

Abelson H and others, “Keys under doormats: Mandating insecurity by requiring government access to all data and communications” (2015) 1(1) Journal of Cybersecurity 69.

Acemoglu D and others, THE PERILS OF HIGH-POWERED INCENTIVES: EVIDENCE FROM COLOMBIA’S FALSE POSITIVES (NBER WORKING PAPER SERIES 2016).

Agarwal AK and Srivastava DK, “Ancient Katapayadi System Sanskrit Encryption Technique Unified” (IEEE July 2014) ⟨http://ieeexplore.ieee.org/document/6884947/⟩.

Akyesilmen N, “CYBERSECURITY AND HUMAN RIGHTS: NEED FOR A PARADIGM SHIFT?” (2016) 1(1) Cyberpolitik Journal 25.

Al Momin MA and Islam MN, “Teleoperated Surgical Robot Security: Challenges and Solutions” in X Hei (ed), *Advances in Web Technologies and Engineering* (IGI Global 2022) ⟨http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-7323-5.ch009⟩.

Alahmari A and Duncan B, “Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence” (IEEE June 2020) ⟨https://ieeexplore.ieee.org/document/9139638/⟩.

Alam MM and others, “A survey on the roles of communication technologies in IoT-Based personalized healthcare applications” (2018) 6 IEEE Access 36611 (Publisher: IEEE).

Alemzadeh H and others, “Adverse events in robotic surgery: A retrospective study of 14 years of fda data” (2016) 11(4) PLoS ONE 1.

Alemzadeh H and others, “Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation” [2016] (395) Proceedings - 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2016 395 (ISBN: 9781467388917).

Alharbi F and others, “The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia” (2021) 21(20) Sensors 6901 ⟨https://www.mdpi.com/1424-8220/21/20/6901⟩.

Allen JG, “Bodies without Organs: Law, Economics, and Decentralised Governance” (2020) 4(1) Stanford Journal of Blockchain Law & Policy.

Almada M, “Two dogmas of technology-neutral regulation” [2024].

Ameen N and others, “Keeping customers’ data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce” (2021) 114 Computers in Human Behavior 106531 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0747563220302831⟩.

Andersen MB and Lookofsky J, *Lærebog i obligationsret* (4th, vol 1, Karnov Group 2010).

Anderson JP, *Computer Security Technology Planning Study. Volume 2:* (techspace rep, Defense Technical Information Center 1972) ⟨http://www.dtic.mil/docs/citations/AD0772806⟩.

Anderson PD, "Review of *Crypto Wars—The Fight for Privacy in the Digital Age: A Political History of Digital Encryption*" [2021] Cryptologia 1 ⟨https://www.tandfonline.com/doi/full/10.1080/01611194.2021.2002977⟩.

Anderson R, *Security engineering: a guide to building dependable distributed systems* (John Wiley & Sons 2020).

Apple Inc, "CSAM Detection - Technical Summary" (Issue: August, 2021) ⟨https://www.apple.com/child-safety/pdf/CSAM%7B%5C_%7DDetection%7B%5C_%7DTechnical%7B%5C_%7DSummary.pdf⟩.

Arabadjieva K, "A Framework for Interpreting the Right to Freedom of Association of Workers and Trade Unions in European Human Rights Law" (Doctor of Philosophy, University of Oxford 2019).

Aranguren Romero JP, Cardona Santofimio JN, and Agudelo Hernández JÁ, "Inhabiting Mourning: Spectral Figures in Cases of Extrajudicial Executions (False Positives) in Colombia" (2021) 40(1) Bulletin of Latin American Research 6 ⟨https://onlinelibrary.wiley.com/doi/10.1111/blar.13104⟩ accessed 3 March 2024.

Ashton M, "Debugging the Real World: Robust Criminal Prosecution in the Internet of Things" (2017) 59(805) Arizona Law Review ⟨http://arizonalawreview.org/pdf/59-3/59arizlrev805.pdf⟩.

Ashworth A, "Self-Incrimination in European Human Rights Law - A Pregnant Pragmatism" (2008) 30(3) Cardozo Law Review.

Askeland B and others, *Basic Questions of Tort Law from a Comparative Perspective* (Jan Sramek Verlag 2015) ⟨https://library.oapen.org/handle/20.500.12657/33062⟩.

Aslam T, Krsul I, and Spafford EH, "Use of A Taxonomy of Security Faults" [1996] Proceedings of the 19th National Information Systems Security Conference 551.

Aston V, "State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives" (2017) 8(1).

Athalye A, Inverting PhotoDNA (2021) ⟨https://www.anishathalye.com/2021/12/20/inverting-photodna/⟩.

Aysu A and others, "Horizontal side-channel vulnerabilities of post-quantum key exchange protocols" (IEEE April 2018) ⟨https://ieeexplore.ieee.org/document/8383894/⟩.

Baboulene G, "Has the elastic interpretation of human rights law led to the 'living instrument' approach to the ECHR interpretation being inherently flawed?" (2023) 48 Exeter Law Review.

Backman S, "Risk vs. threat-based cybersecurity: the case of the EU" (2023) 32(1) European Security 85 ⟨https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2069464⟩ accessed 24 May 2024.

Baker JH, "English Law and the Renaissance" (1985) 44(1) Cambridge Law Journal 46.

Barnett RE, "Foreword: Four Senses of the Public Law-Private Law Distinction" (1986) 9(2) Harvard Journal of Law & Public Policy 11.

Bauer JM and Van Eeten MJG, "Cybersecurity: Stakeholder incentives, externalities, and policy options" (2009) 33(10-11) Telecommunications Policy 706.

Beglinger C, "A Broken Theory : The Malfunction Theory of Strict Products Liability and the Need for a New Doctrine in the Field of Surgical Robotics" (2019) 104(2) Minnesota Law Review 1041.

Behan C, "Embracing and Resisting Prisoner Enfranchisement: A Comparative Analysis of the Republic of Ireland and the United Kingdom" (2014) 11 IRISH PROBATION JOURNAL.

Belfanti C, "Guilds, Patents, and the Circulation of Technical Knowledge: Northern Italy during the Early Modern Age" (2004) 45(3) Technology and Culture 569 ⟨http://muse.jhu.edu/content/crossref/journals/technology_and_culture/v045/45.3belfanti.html⟩.

Bellare M, *A Concrete-Security Analysis of the Apple PSI Protocol* (techspace rep, Apple 2021) ⟨https://www.apple.com/child-safety/pdf/Alternative%7B%5C_%7DSecurity%7B%5C_%7DProof%7B%5C_%7Dof%7B%5C_%7DApple%7B%5C_%7DPSI%7B%5C_%7DSystem%7B%5C_%7DMihir%7B%5C_%7DBellare.pdf⟩.

Bergeles C and Yang GZ, "From passive tool holders to microsurgeons: Safer, smaller, smarter surgical robots" (2014) 61(5) IEEE Transactions on Biomedical Engineering 1565.

Berger M, "Europeanizing Self-Incrimination: The Right to Remain Silent in the European Court of Human Rights" (2006) 12(2) Columbia Journal of European Law.

— "Self-Incrimination and the European Court of Human Rights: Procedural Issues in the Enforcement of the Right to Silence" (2007) 514 European Human Law Review.

Bernitz U, "What is Scandinavian Law?" (2007) 50(1) Scandinavian studies in law.

Bertens RM and Vonk RA, "Small steps, big change. Forging a public-private health insurance system in the Netherlands" (2020) 266 Social Science & Medicine 113418 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0277953620306377⟩.

Besson S, "European human rights, supranational judicial review and democracy : thinking outside the judicial box" in *Human rights protection in the European legal order : The interaction between the European and the national courts* (Intersentia 2011).

Bhowmick A and others, *The Apple PSI System* (techspace rep, 2021).

Biasin E and Kamenjasevic E, "Cybersecurity of Medical Devices: Regulatory Challenges in the EU" in *The Future of Medical Device Regulation: Innovation and Protection* (2020).

Biasin E and Kamenjašević E, "Open Source Hardware and Healthcare Collaborative Platforms: Common Legal Challenges" (2020) 4(1) Journal of Open Hardware 1.

Bignami F, "From Expert Administration to Accountability Network: A New Paradigm for Comparative Administrative Law" (2011) 59(4) American Journal of Comparative Law 859 ⟨https://academic.oup.com/ajcl/article-lookup/doi/10.5131/AJCL.2010.0031⟩.

Binns R, "Data protection impact assessments: a meta-regulatory approach" (2017) 7(1) International Data Privacy Law 22 ⟨https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipw027⟩ accessed 26 February 2024.

Black J, "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World" (2001) 54(1) Current Legal Problems 103 ⟨https://academic.oup.com/clp/article-lookup/doi/10.1093/clp/54.1.103⟩.

"Critical Reflections on Regulation", in J Black and F Haines (eds), *Crime and Regulation* (1st edn, Routledge November 2017).

Blaze M and Labs T, "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks" [2002] 12.

Bleichenbacher D, Kiayias A, and Yung M, "Decoding of Interleaved Reed Solomon Codes over Noisy Data" (ISSN: 16113349, 2003) vol Lecture No.

Boeke S, "National cyber crisis management: Different European approaches" (2018) 31(3) Governance 449 ⟨https://onlinelibrary.wiley.com/doi/10.1111/gove.12309⟩.

Bonaci T and others, "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots" [2015] 1 (_eprint: 1504.04339) ⟨http://arxiv.org/abs/1504.04339⟩.

Boyens J and others, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (techspace rep, National Institute of Standards and Technology 2021) ⟨https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf⟩.

Brand O, "Conceptual Comparisons: Towards a Coherent Methodology of Comparative Legal Studies" (2007) 32(2) Brooklyn Journal of International Law.

Bräunlich K and others, "Linking loose ends: An interdisciplinary privacy and communication model" (2020) 23(6) New Media & Society.

"The Role of Deterrence in the Formulation of Criminal Law Rules: At Its Worst When Doing Its Best" (2003) 91(5) Georgetown Law Journal (Brooks T ed 949 ⟨https://www.taylorfrancis.com/books/9781351944991⟩.

Brown I, *ONLINE FREEDOM OF EXPRESSION, ASSEMBLY, ASSOCIATION AND THE MEDIA IN EUROPE* (Report, Council of Europe 2013).

Brownsword R, "The shaping of our on-line worlds: getting the regulatory environment right" (2012) 20(4) International Journal of Law and Information Technology 249 ⟨https://academic.oup.com/ijlit/article-lookup/doi/10.1093/ijlit/eas019⟩.

Brownsword R, "Artificial Intelligence and Legal Singularity: The Thin End of the Wedge, the Thick End of the Wedge, and the Rule of Law" in S Deakin and C Markou (eds), *Is Law Computable?: Critical Perspectives on Law and Artificial Intelligence* (Hart Publishing 2020) ⟨http://www.bloomsburycollections.com/book/is-law-computable-critical-perspectives-on-law-and-artificial-intelligence⟩.

— *Rethinking Law, Regulation, and Technology* (Edward Elgar 2022).

Bullée J.-W and Junger M, "Social Engineering" in TJ Holt and AM Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (Springer International Publishing 2020) ⟨http://link.springer.com/10.1007/978-3-319-78440-3_38⟩.

Burnside MJ and others, "Open-Source Automated Insulin Delivery in Type 1 Diabetes" (2022) 387(10) New England Journal of Medicine 869 ⟨http://www.nejm.org/doi/10.1056/NEJMoa2203913⟩ accessed 30 April 2023.

Burton S and others, "Mind the gaps: Assuring the safety of autonomous systems from an engineering, ethical, and legal perspective" (2020) 279 Artificial Intelligence 103201 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0004370219301109⟩.

Camara C, Peris-Lopez P, and Tapiador JE, "Security and privacy issues in implantable medical devices: A comprehensive survey" (2015) 55 Journal of Biomedical Informatics 272 (Publisher: Elsevier Inc.) ⟨http://dx.doi.org/10.1016/j.jbi.2015.04.007⟩.

Cantudo-Cuenca MR and others, "A better regulation is required in viral hepatitis smartphone applications" (2014) 38(2) Farmacia Hospitalaria 112.

Cappelen C and Dahlberg S, "The Law of Jante and generalized trust" (2018) 61(4) Acta Sociologica 419.

Cardenas AA and others, "Challenges for Securing Cyber physical Systems" (2009) 2009(3) Computer Audit Update 3.

Carley KM, "Computational organizational science and organizational engineering" (2002) 10(5-7) Simulation Modelling Practice and Theory 253 ⟨https://linkinghub.elsevier.com/retrieve/pii/S1569190X02001193⟩.

Carmody S and others, "Building resilient medical technology supply chains with a software bill of materials" (2021) 4(1) npj Digital Medicine 34 ⟨http://www.nature.com/articles/s41746-021-00403-w⟩.

Carr M and Tanczer LM, "UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions" (2018) 3(3) Journal of Cyber Policy 430.

Casarosa F, “Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act” (2022) 3(1) International Cybersecurity Law Review 115 ⟨https://link.springer.com/10.1365/s43439-021-00043-6⟩.

Cate FH, “The EU Data Protection Directive, Information Privacy, and the Public Interest” (1995) 80(3) Iowa Law Review.

Cernauskas D and Kumiega A, “Back to the future: Cybernetics for safety, quality and cybersecurity” (2022) 29(3) Quality Management Journal 183 ⟨https://www.tandfonline.com/doi/full/10.1080/10686967.2022.2083035⟩.

Charney S and Werner ET, *Cyber Supply Chain Risk Management:Toward a Global Vision of Transparency and Trust* (techspace rep, Microsoft 2011).

Christie J, “The post office horizon it scandal and the presumption of the dependability of computer evidence” (2020) 17(March) Digital Evidence and Electronic Signature Law Review 49.

Chung JJ, “Critical Infrastructure, Cybersecurity, and Market Failure” (2018) 96(2) Oregon Law Review 441.

Clark-Ginsberg A and Slayton R, “Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards” (2019) 46(3) Science and Public Policy 339 ⟨https://academic.oup.com/spp/article/46/3/339/5184558⟩.

Cobbe J, “Administrative law and the machines of government: Judicial review of automated public-sector decision-making” (2019) 39(4) Legal Studies 636.

— “Data protection , ePrivacy , and the prospects for Apple’s on-device CSAM Detection system in Europe” (2021) ⟨https://osf.io/preprints/socarxiv/rhw8c/⟩.

Coe P, “The Draft Online Safety Bill and the regulation of hate speech: have we opened Pandora’s box?” (2022) 14(1) Journal of Media Law 50 ⟨https://www.tandfonline.com/doi/full/10.1080/17577632.2022.2083870⟩ accessed 27 September 2023.

Cohen F, “Computer Viruses - Theory and Experiment” (1987) 6.1 Computers & Security 22 ⟨all.net/books/virus/⟩.

Cohen JE, “The Regulatory State in the Information Age” (2016) 369(2) Theoretical Inquiries in Law.

Coleman EG, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton University Press 2013).

Commission E, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (2022) ⟨https://ec.europa.eu/home-affairs/system/files/2022-05/Proposal%20for%20a%20Regulation%20laying%20down%20rules%20to%20prevent%20and%20combat%20child%20sexual%20abuse%7B%5C_%7Den%7B%5C_%7D0.pdf⟩.

— Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (2022).

Coppersmith D and Sudan M, “Reconstructing curves in three (and higher) dimensional space from noisy data” [2003] Conference Proceedings of the Annual ACM Symposium on Theory of Computing 136 (ISBN: 1581136749).

Corinne Reichert, China reportedly scans tourists’ phones by installing malware (Publication Title: CNET, 2019) ⟨https://www.cnet.com/tech/mobile/china-is-reportedly-scanning-tourists-phones-with-malware/⟩.

Cosgrove L and others, “Digital phenotyping and digital psychotropic drugs: Mental health surveillance tools that threaten human rights” (2020) 22(2) Health and Human Rights 33.

Creazza A and others, “Who cares? Supply chain managers’ perceptions regarding cyber supply chain risk management in the digital transformation era” (2022) 27(1) Supply Chain Management 24.

Cullen A and Wheatley S, "The Human Rights of Individuals in De Facto Regimes under the European Convention on Human Rights" (2013) Human Rights Law Review(13) 4.

D'Souza R, "When Unreason Masquerades as Reason: Can Law Regulate Trade and Networked Communication Ethically?" in *The Handbook of Communication Ethics* (Routledge 2011).

Dahlen ØP and Skirbekk H, "How trust was maintained in Scandinavia through the first crisis of modernity" (2021) 26(1) Corporate Communications: An International Journal 23.

Dambrogio J and others, "Unlocking history through automated virtual unfolding of sealed documents imaged by X-ray microtomography" (2021) 12(1) Nature Communications 1184 ⟨https://www.nature.com/articles/s41467-021-21326-w⟩.

Datta P, "*Hannibal at the gates* : Cyberwarfare & the Solarwinds sunburst hack" [2021] Journal of Information Technology Teaching Cases 204388692199312 ⟨http://journals.sagepub.com/doi/10.1177/2043886921993126⟩.

— "*Hannibal at the gates* : Cyberwarfare & the Solarwinds sunburst hack" (2022) 12(2) Journal of Information Technology Teaching Cases 115 ⟨http://journals.sagepub.com/doi/10.1177/2043886921993126⟩ accessed 2 September 2023.

Degli-Esposti S and Ferrándiz EM, "A Year after GDPR: Cybersecurity is the Elephant in the Artificial Intelligence Room" (2021) 32(1) European Business Law Review 24.

Deibert RJ, "Toward a Human-Centric Approach to Cybersecurity" (2018) 32(4) Ethics & International Affairs 411 ⟨https://www.cambridge.org/core/product/identifier/S0892679418000618/type/journal_article⟩.

Dellinger JC and Hoffman D, "You Are Being Scanned" (2022) 106(3) Judicature.

Den Butter FAG and Mosch RHJ, "Trade, Trust and Transaction Costs" (2003) 3 TI Discussion Paper.

Dezalay Y and Garth B, "From the Cold War to Kosovo: The Rise and Renewal of the Field of International Human Rights" (2006) 2(1) Annual Review of Law and Social Science 231 ⟨https://www.annualreviews.org/doi/10.1146/annurev.lawsocsci.2.032406.145708⟩.

Dhanani NH and others, "The Evidence Behind Robot-Assisted Abdominopelvic Surgery" (2021) 174(8) Annals of Internal Medicine 1100.

Dieter M and others, "Pandemic platform governance: Mapping the global ecosystem of COVID-19 response apps" (2021) 10(3) Internet Policy Review ⟨https://policyreview.info/articles/analysis/pandemic-platform-governance-mapping-global-ecosystem-covid-19-response-apps⟩.

Dillon JT, "The Multidisciplinary Study of Questioning" (1982) 74(2) Journal of Educational Psychology 147.

Dittel A, "The UK's Online Safety Bill: The day we took a stand against serious online harms or the day we lost our freedoms to platforms and the state?" (2022) 5.

Dodig-Crnkovic G, "Scientific Methods in Computer Science" [2002] Proceedings of the Conference for the Promotion of Research in IT at New Universities and at University Colleges in Sweden, Skövde, Suecia 7.

Donalds C and Osei-Bryson K.-M, "Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents" (2020) 51 International Journal of Information Management 102056 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0268401218312544⟩ accessed 1 March 2024.

Dong C and others, "Hardware Trojans in Chips: A Survey for Detection and Prevention" (2020) 20(18) Sensors 5165 ⟨https://www.mdpi.com/1424-8220/20/18/5165⟩.

Donnelly J, "Human Rights as Natural Rights" (1982) 4(3) Human Rights Quarterly 391.

Dooley JF, “Cryptology Before 1500 – A Bit of Magic” in *History of Cryptography and Cryptanalysis* (Series Title: History of Computing, Springer International Publishing 2018) ⟨http://link.springer.com/10.1007/978-3-319-90443-6_2⟩.

— *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms* (History of Computing, Springer International Publishing 2018) ⟨http://link.springer.com/10.1007/978-3-319-90443-6⟩.

— “The Black Chambers: 1500–1776”, in *History of Cryptography and Cryptanalysis* (Series Title: History of Computing, Springer International Publishing 2018) ⟨http://link.springer.com/10.1007/978-3-319-90443-6_3⟩.

Dooms M, “Orphan medical devices have come a long way” (2023) 18(1) Orphanet Journal of Rare Diseases 71 ⟨https://ojrd.biomedcentral.com/articles/10.1186/s13023-023-02685-7⟩ accessed 10 October 2023.

Dror Y, “Law and social change” (1959) 33(4) Tulane Law Review 787.

Duan C, “OF MONOPOLIES AND MONOCULTURES: THE INTERSECTION OF PATENTS AND NATIONAL SECURITY” (2020) 36(4) Santa Clara High Technology Law Journal 39.

Dunn Cavelty M and Smeets M, “Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority” (2023) 30(7) Journal of European Public Policy 1330 ⟨https://www.tandfonline.com/doi/full/10.1080/13501763.2023.2173274⟩ accessed 24 May 2024.

Dürr H, “Vild statistik på sygehus: Robot står bag 1000 operationer” [2019] JydskeVestkysten ⟨https://jv.dk/aabenraa/vild-statistik-paa-sygehus-robot-staar-bag-1000-operationer⟩.

Duzenci A, Kitapci H, and Gok MS, “The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior” (2023) 13(15) Applied Sciences 8731 ⟨https://www.mdpi.com/2076-3417/13/15/8731⟩.

Dworkin R, *Law’s Empire* (1st edn, Harvard University Press 1986).

Eckhardt P and Kotovskaia A, “The EU’s cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive” [2023] International Cybersecurity Law Review.

Economides N and Lianos I, “Restrictions on Privacy and Exploitation in the Digital Economy: A Competition Law Perspective” [2019] CLES Research Paper Series.

Eggers S, “A novel approach for analyzing the nuclear supply chain cyber-attack surface” (2021) 53(3) Nuclear Engineering and Technology 879 (Publisher: Elsevier Ltd) ⟨https://doi.org/10.1016/j.net.2020.08.021⟩.

Eggers SL, “The nuclear digital I&C system supply chain cyber-attack surface” (2020) 122(June) Transactions of the American Nuclear Society 119.

Ellis JH, “THE HISTORY OF NON-SECRET ENCRYPTION” (1999) 23(3) Cryptologia 267 ⟨http://www.tandfonline.com/doi/abs/10.1080/0161-119991887919⟩.

Elsayed GF, Sohl-Dickstein J, and Goodfellow I, “Adversarial reprogramming of neural networks” [2019] 7th International Conference on Learning Representations, ICLR 2019 1 (_eprint: 1806.11146).

Escobar Veas J, “A Comparative Analysis of the Case Law of the European Court of Human Rights on the Right against Self-Incrimination” (2022) 8(2) Revista Brasileira de Direito Processual Penal ⟨https://revista.ibraspp.com.br/RBDPP/article/view/675⟩ accessed 28 September 2023.

Europe C of, European Convention on Human Rights ⟨https://www.echr.coe.int/Documents/Convention%7B%5C_%7DENG.pdf⟩.

Evald J, *Juridisk teori, metode og videnskab* (2nd, Jurist- og økonomforbundets Forlag 2020).

Eyben B von and Isager H, *Lærebog i erstatningsret* (7th, Jurist- og økonomforbundets Forlag 2013).

Ezzamel M and Hoskin K, “Retheorizing accounting, writing and money with evidence from Mesopotamia and ancient Egypt” (2002) 13(3) Critical Perspectives on Accounting 333 ⟨https://linkinghub.elsevier.com/retrieve/pii/S1045235401905003⟩.

Falliere N, Murchu LO, and Chien E, *W32.Stuxnet Dossier* (techspace rep, 1.4, Symantec 2011).

Fanning B, Kloc-Nowak W, and Lesińska M, "Polish migrant settlement without political integration in the United Kingdom and Ireland: a comparative analysis in the context of Brexit and thin European citizenship" (2021) 59(1) International Migration 263 ⟨https://onlinelibrary.wiley.com/doi/10.1111/imig.12758⟩ accessed 19 February 2023.

Farran S and Orlcfl E, "The Continuing Relevance of Comparative Law and Comparative Legal Studies" (2019) 6(2) Journal of International and Comparative Law.

Filippi PD and Hassan S, "Blockchain technology as a regulatory technology: From code is law to law is code" [2016] First Monday ⟨https://firstmonday.org/ojs/index.php/fm/article/view/7113⟩ accessed 2 February 2024.

Finkelstein JJ, "Sex Offenses in Sumerian Laws" (1966) 86(4) Journal of the American Oriental Society 355 ⟨https://www.jstor.org/stable/596493?origin=crossref⟩.

Fosch-Villaronga E and Millard C, "Cloud robotics law and regulation: Challenges in the governance of complex and dynamic cyber–physical ecosystems" (2019) 119 Robotics and Autonomous Systems 77 (Publisher: Elsevier B.V.) ⟨https://doi.org/10.1016/j.robot.2019.06.003⟩.

Frankenberg G, "Critical Comparisons: Re-thinking Comparative Law" in *Legal Theory and the Legal Academy* (Taylor & Francis 2010).

Frankot E, "Medieval Maritime Law from Oléron to Wisby: Jurisdictions in the Law of the Sea" in J Pan-Montojo and F Pedersen (eds), *Communities in European history : representations, jurisdictions, conflicts* (Edizioni Plus – Pisa University Press 2007).

Fraser AG and others, "The need for transparency of clinical evidence for medical devices in Europe" (2018) 392(10146) The Lancet 521.

Friedman LM and Ladinsky J, "Social Change and the Law of Industrial Accidents" (1967) 50 Columbia Law Review 50.

Frosini JO, "Is Brexit Ripping up the Unwritten Constitution of the United Kingdom?" (2019) 11(1) Italian Journal of Public Law.

Fu K, "Trustworthy medical device software" (2011) vol 510 ⟨http://www.cs.ucsb.edu/%7B~%7Dsherwood/cs290/papers/fu.pdf⟩.

Fu K and others, "Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things" [2020] Computing Community Consortium ⟨http://arxiv.org/abs/2008.00017⟩.

Fussey P and Sandhu A, "Surveillance arbitration in the era of digital policing" (2022) 26(1) Theoretical Criminology 3.

Gallese C, "Legal Issues of the Use of Chatbot Apps for Mental Health Support" in A González-Briones and others (eds), *Highlights in Practical Applications of Agents, Multi-Agent Systems, and Complex Systems Simulation. The PAAMS Collection* (Series Title: Communications in Computer and Information Science, Springer International Publishing 2022) vol 1678 ⟨https://link.springer.com/10.1007/978-3-031-18697-4_21⟩ accessed 25 June 2023.

Gardner J and Warren N, "Learning from deep brain stimulation: the fallacy of techno-solutionism and the need for 'regimes of care'" (2019) 22(3) Medicine, Health Care and Philosophy 363 (ISBN: 0123456789 Publisher: Springer Netherlands) ⟨http://dx.doi.org/10.1007/s11019-018-9858-6⟩.

Geierhaas L and others, "Attitudes towards Client-Side Scanning for CSAM, Terrorism, Drug Trafficking, Drug Use and Tax Evasion in Germany" (IEEE May 2023) ⟨https://ieeexplore.ieee.org/document/10179417/⟩ accessed 28 September 2023.

Geva B, “From Commodity to Currency in Ancient History–On Commerce, Tyranny, and the Modern Law of Money” (1987) 25(1) Osgoode Hall Law Journal 115.

Gharib M, “Privacy and Informational Self-determination Through Informed Consent: The Way Forward” (2022) 13106 LNCS Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 171 (ISBN: 9783030954833).

Gilbert S and others, “Large language model AI chatbots require approval as medical devices” [2023] Nature Medicine ⟨https://www.nature.com/articles/s41591-023-02412-6⟩ accessed 10 October 2023.

Gillespie AA, *Cybercrime: Key issues and debates* (Routledge 2015).

Gilling D and others, “Powers, liabilities and expertise in community safety: Comparative lessons for ‘urban security’ from the United Kingdom and the Republic of Ireland” (2013) 10(3) European Journal of Criminology 326 ⟨http://journals.sagepub.com/doi/10.1177/1477370813482612⟩ accessed 19 February 2023.

Gilmore G, “From Tort to Contract: Industrialization and the Law” (1977) 86(4) The Yale Law Journal 788 ⟨https://www.jstor.org/stable/795645?origin=crossref⟩.

Gomard B, Godsk Pedersen HV, and Ørgaard A, *Almindelig kontraktsret* (4th, Jurist- og økonomforbundets Forlag 2015).

Gómez-González E and others, “Artificial intelligence in medicine and healthcare: a review and classification of current and near-future applications and their ethical and social Impact” (_eprint: 2001.09778, 2020) ⟨http://arxiv.org/abs/2001.09778⟩.

Gong X and others, “Model Extraction Attacks and Defenses on Cloud-Based Machine Learning Models” (2020) 58(12) IEEE Communications Magazine 83 ⟨https://ieeexplore.ieee.org/document/9311938/⟩.

Grewal D and others, “The future of technology and marketing: a multidisciplinary perspective” (2020) 48(1) Journal of the Academy of Marketing Science 1 ⟨http://link.springer.com/10.1007/s11747-019-00711-4⟩ accessed 17 December 2023.

Griffiths A, “Law, Space, and Place: Reframing Comparative Law and Legal Anthropology” (2009) 34(02) Law & Social Inquiry 495 ⟨https://www.cambridge.org/core/product/identifier/S0897654600006067/type/journal_article⟩.

Gunatilleke G, “Justifying Limitations on the Freedom of Expression” (2021) 22(1) Human Rights Review 91 ⟨http://link.springer.com/10.1007/s12142-020-00608-8⟩ accessed 14 February 2024.

Gyenes R, “A Voluntary Cybersecurity Framework Is Unworkable- Government Must Crack the Whip” (2014) 14(2) Pittsburgh Journal of Technology Law and Policy 293.

Ha G and others, “Threat Model and Defense Scheme for Side-Channel Attacks in Client-Side Deduplication” (2023) 28(1) Tsinghua Science and Technology 1 ⟨https://ieeexplore.ieee.org/document/9837022/⟩ accessed 23 September 2023.

Haber E and Zarsky T, “Cybersecurity for Infrastructure: A Critical Analysis” (2017) 44(2) Florida State University Law Review.

Halperin D and others, “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses” [2008] Proceedings - IEEE Symposium on Security and Privacy 129 (ISBN: 9780769531687).

Hantke F and others, “Where Are the Red Lines? Towards Ethical Server-Side Scans in Security and Privacy Research” (2024).

Hanus B, Wu YA, and Parrish J, “Phish Me, Phish Me Not” (2022) 62(3) Journal of Computer Information Systems 516 ⟨https://www.tandfonline.com/doi/full/10.1080/08874417.2020.1858730⟩ accessed 16 February 2023.

Harlow C, “Public and Private Law: Definition without Distinction” (1980) 43(3) Modern Law Review 241.

Harris MA and Martin R, "Promoting Cybersecurity Compliance" in I Vasileiou and S Furnell (eds), *Advances in Information Security, Privacy, and Ethics* (IGI Global February 2019) ⟨https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-7847-5.ch004⟩ accessed 1 March 2024.

Hein D, Morozov S, and Saiedian H, "A survey of client-side Web threats and counter-threat measures: Client-side Web threats and counter-threat measures" (2012) 5(5) Security and Communication Networks 535 ⟨https://onlinelibrary.wiley.com/doi/10.1002/sec.349⟩ accessed 23 September 2023.

Hellegren ZI, "A history of crypto-discourse: encryption as a site of struggles to define internet freedom" (2017) 1(4) Internet Histories 285 ⟨https://www.tandfonline.com/doi/full/10.1080/24701475.2017.1387466⟩.

Hilaire-Perez L and Verna C, "Dissemination of Technical Knowledge in the Middle Ages and the Early Modern Era: New Approaches and Methodological Issues" (2006) 47(3) Technology and Culture 536 ⟨http://muse.jhu.edu/content/crossref/journals/technology_and_culture/v047/47.3hilaire-perez.html⟩.

Hildebrandt M, "Code-driven Law: Freezing the Future and Scaling the Past" in S Deakin and C Markou (eds), *Is Law Computable?: Critical Perspectives on Law and Artificial Intelligence* (Hart Publishing 2020) ⟨http://www.bloomsburycollections.com/book/is-law-computable-critical-perspectives-on-law-and-artificial-intelligence⟩.

Hirsch DD, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation" (2011) 34(2) Seattle University Law Review.

Hockstein NG and others, "A history of robots: From science fiction to surgical robotics" (2007) 1(2) Journal of Robotic Surgery 113.

Holder C and others, "Robotics and law: Key legal and regulatory implications of the robotics age (part II of II)" (2016) 32(4) Computer Law and Security Review 557 (Publisher: Elsevier Ltd) ⟨http://dx.doi.org/10.1016/j.clsr.2016.05.011⟩.

Holvast J, "History of Privacy" (2009) 298 FIP Advances in Information and Communication Technology.

Hooda A and others, Re-purposing Perceptual Hashing based Client Side Scanning for Physical Surveillance (arXiv:2212.04107 [cs], arXiv December 2022) ⟨http://arxiv.org/abs/2212.04107⟩ accessed 28 September 2023.

Howells G, "Product Liability – A History of Harmonisation" in *Product Liability in Comparative Perspective* (Cambridge University Press 2005).

Hughes K and Richards NM, "The Atlantic divide on privacy and free speech" in *Comparative defamation and privacy law* (Cambridge University Press 2016).

Hupli T, "To Remain or Not to Remain Silent: The Evolution of The Privilege against Self-incrimination Ten Years After Marttinen v. Finland" (2018) 6(2) Bergen Journal of Criminal Law and Criminal Justice 136.

Hurwitz J, "Cyberensuring Security" (2017) 49(5) Connecticut Law Review.

Husa J, Comparative Law and Interdisciplinarity, "Law &" (An Encyclopedia of Interdisciplinary Studies, Hong Kong University 2024).

Hutchinson T, "The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law" [2016] Erasmus Law Review (Taekema S ed ⟨http://www.elevenjournals.com/doi/10.5553/ELR.000055⟩.

Hutchinson T and Duncan N, "Defining and Describing What We Do: Doctrinal Legal Research" (2012) 17(1) Deakin Law Review 83 ⟨https://ojs.deakin.edu.au/index.php/dlr/article/view/70⟩.

Jacob J, Peters M, and Yang TA, "Interdisciplinary Cybersecurity: Rethinking the Approach and the Process" in K.-KR Choo, TH Morris, and GL Peterson (eds), *National Cyber Summit (NCS) Research Track* (Series Title: Advances in Intelligent Systems and Computing, Springer International Publishing 2020) vol 1055 ⟨http://link.springer.com/10.1007/978-3-030-31239-8_6⟩.

Jain S, Cretu A.-M, and Montjoye Y.-A de, "Adversarial Detection Avoidance Attacks: Evaluating the robustness of perceptual hashing-based client-side scanning" [2022] USENIX Security 2022.

Jain S and others, "Deep perceptual hashing algorithms with hidden dual purpose: when client-side scanning does facial recognition" (IEEE May 2023) ⟨https://ieeexplore.ieee.org/document/10179310/⟩ accessed 29 April 2024.

Jaton F, "Assessing biases, relaxing moralism: On ground-truthing practices in machine learning design and application" (2021) 8(1) Big Data and Society.

Jimenez M, "Finding the Good in Holmes's Bad Man" (2011) 79(5) Fordham Law Review 2069.

Jiménez González A, "Law, Code and Exploitation: How Corporations Regulate the Working Conditions of the Digital Proletariat" (2022) 48(2) Critical Sociology 361 ⟨http://journals.sagepub.com/doi/10.1177/08969205211028964⟩.

Johnson G and Shriver S, Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR (2019) ⟨https://www.ssrn.com/abstract=3477686⟩.

Johnson RA and Rostain T, "Tool for surveillance or spotlight on inequality? Big data and the law" (2020) 16 Annual Review of Law and Social Science 453.

Johson R, "The "False Positives" Scandal: Extrajudicial Killings and the Militarization of Domestic Security in Colombia" (Bachelor of Arts degree in International Studies, The University of Mississippi 2011).

Jones HM, "Ideas, History, Technology" (1959) 1(1) Technology and Culture 20 ⟨https://www.jstor.org/stable/3100784?origin=crossref⟩.

Jørgensen RF, "Data and rights in the digital welfare state: the case of Denmark" (2021) 0(0) Information Communication and Society 1 (Publisher: Taylor & Francis) ⟨https://doi.org/10.1080/1369118X.2021.1934069⟩.

Jue J, Shah NA, and Mackey TK, "An Interdisciplinary Review of Surgical Data Recording Technology Features and Legal Considerations" (2020) 27(2) Surgical Innovation 220 ⟨http://journals.sagepub.com/doi/10.1177/1553350619891379⟩.

Kamara I, Misaligned Union laws? A comparative analysis of certification in the Cybersecurity Act and the General Data Protection Regulation (2021).

Kamel Boulos MN and others, "Mobile medical and health apps: state of the art, concerns, regulatory control and certification" (2014) 5(3) Online Journal of Public Health Informatics 1.

Kaufman C, "The Law of International Commercial Transactions (Lex Mercatoria)" (1978) 19(1) Harvard International Law Journal 58.

Kavak H and others, "Simulation for cybersecurity: state of the art and future directions" (2021) 7(1) Journal of Cybersecurity 1 ⟨https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyab005/6170701⟩.

Kaviani S, Han KJ, and Sohn I, "Adversarial Attacks and Defences on AI in Medical Imaging Informatics: A Survey" [2022] Expert Systems With Applications 116815 (Publisher: Elsevier Ltd.) ⟨https://doi.org/10.1016/j.eswa.2022.116815⟩.

Kelemen M, Szabo S, and Vajdová I, "Cybersecurity in the Context of Criminal Law Protection of the State Security and Sectors of Critical Infrastructure" [2018] Challenges to national defence in contemporary geopolitical situation 100 ⟨https://journals.lka.lt/doi/10.47459/cndcgs.2018.14⟩.

Kelsen H, "Pure Theory of Law, The - Its Method and Fundamental Concepts" (1934) 50(4) Quarterly Review.

Kerckhoffs A, "La cryptographie militaire" (1883) IX Journal des sciences militaires 5 ⟨http://www.petitcolas.net/fabien/kerckhoffs/⟩.

Kerstens J and Veenstra S, "Cyber Bullying In The Netherlands: A Criminological Perspective" [2016] (Publisher: Zenodo) ⟨https://zenodo.org/record/55055⟩ accessed 20 February 2023.

Kianpour M, Kowalski SJ, and Øverby H, "Systematically understanding cybersecurity economics: A survey" (2021) 13(24) Sustainability (Switzerland).

Kianpour M, Kowalski SJ, and Øverby H, "Advancing the concept of cybersecurity as a public good" (2022) 116(January) Simulation Modelling Practice and Theory (Publisher: Elsevier B.V.).

Kilovaty I, "Privatized Cybersecurity Law" (2019) 10(4) Irvine Law Review.

King LW (tr), Hammurabi's Code of Laws (1915).

King TC and others, "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions" (2020) 26(1) Science and Engineering Ethics 89 ⟨http://link.springer.com/10.1007/s11948-018-00081-0⟩.

Kleber K and Frahm E, "A Not-so-Great Escape: Crime and Punishment according to a Document from Neo-Babylonian Uruk" (2006) 58(1) Journal of Cuneiform Studies 109 ⟨https://www.journals.uchicago.edu/doi/10.1086/JCS40025226⟩.

Kobara K, "Cyber physical security for Industrial Control Systems and IoT" (2016) E99D(4) IEICE Transactions on Information and Systems 787.

Koltay A, "Defamation on the internet: the role and responsibilities of gatekeepers" in *Comparative Privacy and Defamation* (2020).

Konar S and Cohen MA, "Information As Regulation: The Effect of Community Right to Know Laws on Toxic Emissions" (1997) 32(1) Journal of Environmental Economics and Management 109 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0095069696909559⟩.

Koops B.-J, "Should ICT Regulation Be Technology-Neutral?" in (2006).

Korkka-Knuts H, "Behaviourally informed approach to corporate criminal law: Ethicality as efficiency" (2022) 10(1) Bergen Journal of Criminal Law & Criminal Justice 30 ⟨https://boap.uib.no/index.php/BJCLCJ/article/view/3689⟩.

Kosseff J, "Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System" (2016) 19(2) Chapman Law Review.

— "Defining Cybersecurity Law" (2018) 103(3) Iowa Law Review.

— "Upgrading Cybersecurity Law" [2023] Houston Law Review.

Kramer DB and others, "Ensuring medical device effectiveness and safety: a cross–national comparison of approaches to regulation." (2014) 69(1) Food and Drug Law Journal 1.

Kramer IR, "The Birth of Privacy Law: A Century since Warren and Brandeis" (1990) 39(3) Catholic University Law Review 703.

La RJ, "Role of network topology in cybersecurity" (IEEE December 2014).

Ladeur K.-H, The Theory of Autopoiesis as an Approach to a Better Understanding of Postmodern Law (EUI Working Papers, 1999).

LaGreca E and Boonthum-Denecke C, "Survey on the Insecurity of the Internet of Things" (2017).

Lamas A and others, "Human pose estimation for mitigating false negatives in weapon detection in video-surveillance" (2022) 489 Neurocomputing 488 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0925231221019159⟩.

Landwehr CE and others, "A taxonomy of Computer Program Security Flaws" (1994) 26(3) ACM Computing Surveys (CSUR) 211.

Laskai L and Segal A, *The Encryption Debate in China: 2021 Update* (techspace rep, March, Carnegie Endowment for International Peace 2021) ⟨https://carnegieendowment.org/files/202104-Germany%7B%5C_%7DCountry%7B%5C_%7DBrief.pdf⟩.

Laukyte M, "An Interdisciplinary Approach to Multi-agent Systems: Bridging the Gap between Law and Computer Science" (2013) 22(1) Informatica e diritto.

Lazarovitz L, "Deconstructing the SolarWinds breach" (2021) 2021(6) Computer Fraud & Security 17 ⟨http://www.magonlinelibrary.com/doi/10.1016/S1361-3723%2821%2900065-8⟩ accessed 2 September 2023.

Le HM, Do TN, and Phee SJ, "A survey on actuators-driven surgical robots" (2016) 247 Sensors and Actuators, A: Physical 323 (Publisher: Elsevier B.V.) ⟨http://dx.doi.org/10.1016/j.sna.2016.06.010⟩.

Leahy A, "DEATH BY FIRE IN ANCIENT EGYPT" (1984) 27(2) Journal of the Economic and Social History of the Orient.

Leebron DW, "eeb" [1990] (3) Annual Survey of American Law.

Leenes R and others, "Regulatory challenges of robotics: Some guidelines for addressing legal and ethical issues" (2017) 9(1) Law, Innovation and Technology 1 (Publisher: Taylor & Francis) ⟨https://doi.org/10.1080/17579961.2017.1304921⟩.

Legh-Jones PN, "Products Liability: Consumer Protection in America" (1969) 27(1) The Cambridge Law Journal 54 ⟨https://www.cambridge.org/core/product/identifier/S0008197300088905/type/journal_article⟩ accessed 18 December 2023.

Lessig L, *Code and other laws of cyberspace* (OCLC: ocm42860053, Basic Books 1999).

Leurs K, "Communication rights from the margins: politicising young refugees' smartphone pocket archives" (2017) 79(6-7) International Communication Gazette 674.

Leveson N and Thomas JP, *STPA Handbook* (2018).

Leveson NG, *Safeware: System Safety and Computers* (1., Addison-Wesley Publishing Company, Inc 1995).

Leveson NG, CAST Handbook: How to Learn More from Incidents and Accidents (2019).

Levi-Faur D, "REGULATION & REGULATORY GOVERNANCE" in *Handbook on the Politics of Regulation* (Elgar 2011).

Levmore S, "Rethinking Comparative Law: Variety and Uniformity in Ancient and Modern Tort Law" (1986) 61(2) Tulane Law Review 235.

Li C, Raghunathan A, and Jha NK, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system" [2011] 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2011 150 (ISBN: 9781612846972 Publisher: IEEE).

Liebetrau T, "Problematising EU Cybersecurity: Exploring How the Single Market Functions as a Security Practice" (2024) 62(3) JCMS: Journal of Common Market Studies 705 ⟨https://onlinelibrary.wiley.com/doi/10.1111/jcms.13523⟩ accessed 24 May 2024.

Lin H and others, "Safety-Critical Cyber-Physical Attacks : Analysis, Detection, and Mitigation" [2016] 82 (ISBN: 9781450342773).

Lofaso AM, "Approaching Coal Mine Safety from a Comparative Law and Interdisciplinary Perspective" (2008) 111(1) West Virginia Law Review.

Lorenc JA, "John of Freiburg and the Usury Prohibition in the Late Middle Ages: A Study in the Popularization of Medieval Canon Law" (Doctor of Philosophy, University of Toronto 2013).

Lukina A, "Making Sense of Evil Law" [2022] SSRN Electronic Journal ⟨https://www.ssrn.com/abstract=4180729⟩.

Lum JW and others, "A Real-World Prospective Study of the Safety and Effectiveness of the Loop Open Source Automated Insulin Delivery System" (2021) 23(5) Diabetes Technology & Therapeutics 367 ⟨https://www.liebertpub.com/doi/10.1089/dia.2020.0535⟩ accessed 30 April 2023.

Luskin R, "'Caring about Corporate 'Due Care': Why Criminal Respondeat Superior Liability Outreaches Its Justification" (2020) 57(2) American Criminal Law Review 29.

Luzan P and others, "The Methodology for Assessment of Engineering Students Outcomes" (IEEE September 2021) ⟨https://ieeexplore.ieee.org/document/9598666/⟩.

Lyon D, *State and Surveillance* (techspace rep, Centre for International Governance Innovation 2019).

— *Pandemic Surveillance* (John Wiley & Sons 2021).

Lyons JS, "Powerloom Profitability and Steam Power Costs: Britain in the 1830s" (1987) 24(4) Explorations in Economic History.

Magnetti DL, "Oath-functions and the oath process in the civil and criminal law of the ancient near east" (1979) 5(1) Brooklyn Journal of International Law 1.

Mantelero A, "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment" (2018) 34(4) Computer Law & Security Review 754 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364918302012⟩ accessed 26 February 2024.

Mantelero A and Esposito MS, "An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems" (2021) 41 Computer Law & Security Review 105561 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364921000340⟩ accessed 26 February 2024.

Marelli M, "The SolarWinds hack: Lessons for international humanitarian organizations" (2022) 104(919) International Review of the Red Cross 1267 ⟨https://www.cambridge.org/core/product/identifier/S1816383122000194/type/journal_article⟩.

Markopoulou D, Papakonstantinou V, and Hert P de, "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation" (2019) 35(6) Computer Law & Security Review 105336 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364919300512⟩.

Marr K, "You're Only as Good as Your Tax Software: The Tax Court's Wrongful Approval of the Turbotax Defense in Olsen v. Commissioner" (2012) 81(2) University of Cincinnati Law Review 709.

Martínez J and Durán JM, "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study" (2021) 11(5) International Journal of Safety and Security Engineering 537 ⟨https://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.110505⟩.

Martini M and Kemper C, "Cybersicherheit von Gehirn-Computer-Schnittstellen" [2022] International Cybersecurity Law Review (ISBN: 1281121339).

Massacci F, Jaeger T, and Peisert S, "SolarWinds and the Challenges of Patching: Can We Ever Stop Dancing With the Devil?" (2021) 19(2) IEEE Security & Privacy 14 ⟨https://ieeexplore.ieee.org/document/9382358/⟩ accessed 2 September 2023.

Mattessich R, "Accounting and the Input-Output Principle in the Prehistoric and Ancient World" (1989) 25(2) Abacus 74 ⟨https://onlinelibrary.wiley.com/doi/10.1111/j.1467-6281.1989.tb00222.x⟩.

Mayanja SJ, "Circumstantial Evidence and Its Admissibility in Criminal Proceedings: A Comparative Analysis of the Common Law and Islamic Law Systems" (2017) 67 Journal of Law, Policy and Globalization.

Mayer J and Kulshrestha A, Opinion: We built a system like Apple's to flag child sexual abuse material — and concluded the tech was dangerous (Publication Title: The Washington Post, 2021) ⟨https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/⟩.

McBride M, Carter L, and Warkentin M, *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies* (Prepared by RTI International – Institute for Homeland Security Solutions under contract 3-312-0212782, 2012).

Mefenza T and others, "Polynomial interpolation of the generalized Diffie–Hellman and Naor–Reingold functions" (2019) 87 Designs, Codes and Cryptography 75 (ISBN: 1062301804861).

Or-Meir O and others, "Dynamic Malware Analysis in the Modern Era—A State of the Art Survey" (2020) 52(5) ACM Computing Surveys 1 ⟨https://dl.acm.org/doi/10.1145/3329786⟩.

Meland PH and others, "A Retrospective Analysis of Maritime Cyber Security Incidents" (2021) 15(3) TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation 519 ⟨http://www.transnav.eu/Article_A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents_Meland,59,1144.html⟩.

Menski W, "Sanskrit Law: Excavating Vedic Legal Pluralism" [2010] SSRN Electronic Journal ⟨http://www.ssrn.com/abstract=1621384⟩.

Merli F, "Principle of Legality and the Hierarchy of Norms" [2015] Southern California Law Review.

Merrymant JH, "The Public Law-Private Law Distinction in European and American Law" (1968) 17(1) Journal of Public Law 3.

Mgbeoji I, "The Juridical Origins of the International Patent System: Towards a Historiography of the Role of Patents in Industrialization" (2003) 5(2) Journal of the History of International Law / Revue d'histoire du droit international 403 ⟨https://brill.com/view/journals/jhil/5/2/article-p403_7.xml⟩.

Michaels R, "Comparative Law by Numbers? Legal Origins Thesis, Doing Business Reports, and the Silence of Traditional Comparative Law" (2009) 57(4) American Journal of Comparative Law 765 ⟨https://academic.oup.com/ajcl/article-lookup/doi/10.5131/ajcl.2008.0022⟩.

Miller JF, *Supply Chain Attack Framework and Attack Patterns* (techspace rep, December 2013, MITRE 2013) ⟨https://apps.dtic.mil/sti/pdfs/ADA610495.pdf⟩.

Minssen T, Mimler M, and Mak V, "When Does Stand-Alone Software Quality as a Medical Device in the European Union? - The CJEU's Decision in SNITEM and What it Implies for the Next Generation of Medical Devices" (2020) 28(3) Medical Law Review 615.

Mishra A and Mishra D, "Cyber Stalking: A Challenge for Web Security" in *Examining the Concepts, Issues, and Implications of Internet Trolling* (2013).

Mitsch WJ and Jørgensen SE, "Ecological engineering: A field whose time has come" (2003) 20(5) Ecological Engineering 363 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0925857403000600⟩.

Mohammed D, "Cybersecurity Compliance in the Financial Sector" (2015) 20(1).

Morenas J de las and others, "Security Experiences in IoT based applications for Building and Factory Automation" (IEEE February 2020) ⟨https://ieeexplore.ieee.org/document/9067229/⟩.

Morgan FW and Boedecker KA, "A historical view of strict liability for product-related injuries" (1996) 16(1) Journal of Macromarketing 103.

Morris J, "Surveillance By Amazon: The Warrant Requirement, Tech Exceptionalism, & Ring Security" (2021) 27(1) Boston University Journal of Science and Technology Law 237 (ISBN: 3600279793).

Mozaffari-Kermani M and others, "Systematic Poisoning Attacks on and Defenses for Machine Learning in Healthcare" (2015) 19(6) IEEE Journal of Biomedical and Health Informatics 1893 ⟨http://ieeexplore.ieee.org/document/6868201/⟩.

"The Technology and Economics of Coinage Debasements in Medieval and Early Modern Europe: with Special Reference to the Low Countries and England", in JH Munro (ed), *Money in the Pre-Industrial World* (1st,

Routledge October 2015) ⟨https://www.taylorfrancis.com/books/9781317321910/chapters/10.4324/9781315655383-8⟩.

Nair A, "Internet Content Regulation: Is a Global Community Standard a Fallacy or the Only Way Out?" (2007) 21(1) International Review of Law, Computers & Technology 15.

Nau RF, "DE FINETTI WAS RIGHT: PROBABILITY DOES NOT EXIST" (2001) 51 Theory and Decision 89 ⟨https://link.springer.com/article/10.1023/A:1015525808214%7B%5C#%7Dciteas⟩.

Neubert C and others, *There is no Software, there are just Services* (Kaldrack I and Leeker M eds, 2015).

Nguyen HD and others, "Industrial Internet of Things, Big Data, and Artificial Intelligence in the Smart Factory: a survey and perspective" [2019] 6.

Nicol DM and Mallapura V, "Modeling and Analysis of Stepping Stone Attacks" [2014] Proceedings of the 2014 Winter Simulation Conference 3036 (ISBN: 9781119130536).

Niemeyer G, Preusche C, and Hirzinger G, "Telerobotics" in *Springer Handbook of Robotics* (Section: 31. 2008).

Nordrum JCF and Ikdahl I, "En vidunderlig ny velferdsstat? Rettsstaten møter den digitale velferdsforvaltningen" no (2022) 25(3) Tidsskrift for velferdsforskning.

NSF, *Cyber-Physical Systems* (techspace rep, National Science Foundation 2014).

Ohm P, "The argument against technology-neutral surveillance laws" [2010] Texas Law Review.

Ong JS and others, "Medical Technology: A Systematic Review on Medical Devices Utilized forEpilepsy Prediction and Management" en (2022) 20(5) Current Neuropharmacology 950 ⟨https://www.eurekaselect.com/197799/article⟩ accessed 19 October 2024.

Osman M, Nudges: four reasons to doubt popular technique to shape people's behaviour (2022) ⟨https://theconversation.com/nudges-four-reasons-to-doubt-popular-technique-to-shape-peoples-behaviour-174359⟩.

Oster J, "Code is code and law is law—the law of digitalization and the digitalization of law" (2021) 29(2) International Journal of Law and Information Technology 101 ⟨https://academic.oup.com/ijlit/article/29/2/101/6313392⟩.

Pacella JM, "The Cybersecurity Threat: Compliance and the Role of Whistleblowers" (2016) 11(1) Brooklyn Journal of Corporate, Financial & Commercial Law.

Pagh R and Rodler FF, "Cuckoo Hashing" in *BRICS Report Series* (ISSN: 0909-0878, August, 2001) ⟨http://link.springer.com/10.1007/3-540-44676-1%7B%5C_%7D10⟩.

Pan J, Qian C, and Ringerud M, "Signed Diffie-Hellman Key Exchange with Tight Security" in *Topics in Cryptology – CT-RSA 2021* (2021).

Papp D, Ma Z, and Buttyan L, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy" [2015] 2015 13th Annual Conference on Privacy, Security and Trust, PST 2015 145 (ISBN: 9781467378284).

Parker L and others, "A health app developer's guide to law and policy: A multi-sector policy analysis" (2017) 17(1) BMC Medical Informatics and Decision Making 1 (ISBN: 1291101705 Publisher: BMC Medical Informatics and Decision Making).

Pavlova P, "Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups" (2020) 4(11/2020) Peace Human Rights Governance 391 ⟨https://doi.org/10.14658/pupj-phrg-2020-3-4⟩.

Peat D, "Perception and Process: Towards a Behavioural Theory of Compliance" (2022) 13(2) Journal of International Dispute Settlement 179 ⟨https://academic.oup.com/jids/article/13/2/179/6439208⟩.

Peiris GL, "The Admissibility of Evidence Obtained Illegally: A Comparative Analysis" (1981) 13(2) Ottawa Law Review.

Peisert S and others, “Perspectives on the SolarWinds Incident” (2021) 19(2) IEEE Security and Privacy 7.

Pinkas B, The Private Set Intersection (PSI) Protocol of the Apple CSAM Detection System (Publication Title: Decentralized Thoughts, 2021) ⟨https://decentralizedthoughts.github.io/2021-08-29-the-private-set-intersection-psi-protocol-of-the-apple-csam-detection-system/⟩.

Pirie F, “Law as ritual: Evoking an ideal order” en (2024) 14(2) HAU: Journal of Ethnographic Theory 403 ⟨https://www.journals.uchicago.edu/doi/10.1086/730785⟩ accessed 24 September 2024.

Pisaric M, “Communications Encryption as an Investigative Obstacle” (2022) 60(1) Journal of Criminology and Criminal Law 61.

Pljonkin AP, “Vulnerability of the Synchronization Process in the Quantum Key Distribution System” (2019) 9(1) International Journal of Cloud Applications and Computing.

Prokhorenko V, Choo K.-KR, and Ashman H, “Web application protection techniques: A taxonomy” (2016) 60 Journal of Network and Computer Applications 95 ⟨https://linkinghub.elsevier.com/retrieve/pii/S1084804515002908⟩ accessed 23 September 2023.

Prokos J and others, “Squint Hard Enough: Attacking Perceptual Hashing with Adversarial Machine Learning” (2023).

Quarta D and others, “An Experimental Security Analysis of an Industrial Robot Controller” [2017] Proceedings - IEEE Symposium on Security and Privacy 268 (ISBN: 9781509055326).

Rashid Z, Noor U, and Altmann J, “Network Externalities in Cybersecurity Information Sharing Ecosystems” in M Coppola and others (eds), *Economics of Grids, Clouds, Systems, and Services* (Series Title: Lecture Notes in Computer Science, Springer International Publishing 2019) vol 11113 ⟨http://link.springer.com/10.1007/978-3-030-13342-9_10⟩ accessed 1 September 2023.

Reed C, “Taking Sides on Technology Neutrality” (2007) 4(3) SCRIPT-ed 263 ⟨http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp⟩ accessed 29 July 2023.

Reed M, Miller JF, and Popick P, *Supply Chain Attack Patterns : Framework and Catalog* (techspace rep, OFFICE OF THE DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR SYSTEMS ENGINEERING 2014) ⟨https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.648.6043&rep=rep1&type=pdf⟩.

Reidenberg JR, “Lex Informatica: The Formulation of Information Policy Rules through Technology” [1997] (76) Texas Law Review.

Review TIM

bibinitperiodMDS, *First Do No Harm, The report of the Independent Medicines and Medical Devices Safety Review* (techspace rep, 2020).

Rezende IN, “Facial recognition in police hands: Assessing the ‘Clearview case’ from a European perspective” (2020) 11(3) New Journal of European Criminal Law 375.

Rinda P and Rosulek M, “Malicious-Secure private set intersection via dual execution” [2017] Proceedings of the ACM Conference on Computer and Communications Security 1229 (ISBN: 9781450349468).

Rizvi S and others, “Securing the Internet of Things (IoT): A Security Taxonomy for IoT” [2018] Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018 163 (ISBN: 9781538643877 Publisher: IEEE).

Robinson P, “Functional Analysis of Criminal Law” (1993) 88(3) Northwestern University Law Review.

Rolph D, “Liability of internet intermediaries for defamation: beyond publication and innocent dissemination” in *Comparative Privacy and Defamation* (2016, 2020) vol 635.

Roque A, Bush KB, and Degni C, "Security is about control: insights from cybernetics" (ACM April 2016) ⟨https://dl.acm.org/doi/10.1145/2898375.2898379⟩.

Rosenzweig P, "The Law and Policy of Client-Side Scanning" (2020) 58 Joint PIJIP/TLS Research Paper Series.

Ross A, *Om Ret og Retfærdighed* (2nd edn, Gyldendal 2013).

Roth VJ., "How much FDA Medical Device Regulation is required?" (2014) 15(3) North Carolina Journal of Law & Technology.

Roy S and others, "Survey and Taxonomy of Adversarial Reconnaissance Techniques" [2022] ACM Computing Surveys 3538704 ⟨https://dl.acm.org/doi/10.1145/3538704⟩.

Rudin GJ, "Walling off Privacy: Apple's NeuralHash Controversy, the ECPA, the Fourth Amendment, and Encryption" (2023) 21(2) Colorado Technology Law Journal.

Rugwiji TT, "Rereading Narratives of Safety and Security in Ancient Israel from a Pastoral Perspective" (2018) 27(1) Journal for Semitics ⟨https://unisapressjournals.co.za/index.php/JSEM/article/view/3559⟩.

Ruohonen J, "An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union" (2020) 5(2) European Journal for Security Research 349 ⟨http://link.springer.com/10.1007/s41125-019-00053-w⟩.

Sadqi Y and Maleh Y, "A systematic review and taxonomy of web applications threats" (2022) 31(1) Information Security Journal: A Global Perspective 1 ⟨https://www.tandfonline.com/doi/full/10.1080/19393555.2020.1853855⟩ accessed 23 September 2023.

Salcedo JC, "Reflections on the Existence of a Hierarchy of Norms in International Law" (1997) 8(4) European Journal of International Law 583 ⟨https://academic.oup.com/ejil/article-lookup/doi/10.1093/oxfordjournals.ejil.a015608⟩.

Sandeen SK, "Out of thin air: trade secrets, cybersecurity and the wrongful acquisition tort" in T Aplin (ed), *Research Handbook on Intellectual Property and Digital Technologies* (Edward Elgar Publishing January 2020) ⟨https://china.elgaronline.com/view/edcoll/9781785368332/9781785368332.00025.xml⟩ accessed 13 January 2024.

Sayakkara AP and Le-Khac NA, "Forensic insights from smartphones through electromagnetic side-channel analysis" (2021) 9 IEEE Access 13237.

Scarman TRHL, "Human Rights in an Unwritten Constitution" (2012) 2(1) The Denning Law Journal 129 ⟨http://www.ubplj.org/index.php/dlj/article/view/163⟩.

Schafer B, *Legal Tech and Computational Legal Theory* (Publication Title: Law and Technology in a Global Digital Society, 2022).

Schmitz-Berndt S and Chiara PG, "One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive" (2022) 3(2) International Cybersecurity Law Review 289 ⟨https://link.springer.com/10.1365/s43439-022-00058-7⟩ accessed 2 September 2023.

Schmitz-Berndt S and Schiffner S, "Don't tell them now (or at all)–responsible disclosure of security incidents under NIS Directive and GDPR" (2021) 35(2) International Review of Law, Computers and Technology 101 (Publisher: Taylor & Francis) ⟨https://doi.org/10.1080/13600869.2021.1885103⟩.

Schwartz PM, "Privacy and Democracy in Cyberspace" (1999) 52(6) Vanderbilt Law Review 1609.

Sekalala S and others, "Analyzing the human rights impact of increased digital public health surveillance during the COVID-19 crisis" (2020) 22(2) Health and Human Rights 7.

Sellmann JD, "On the Origin of Shang and Zhou Law" (2006) 16(1) Asian Philosophy 49 ⟨https://www.tandfonline.com/doi/full/10.1080/09552360500491866⟩.

Sen A, "Speaking of Freedom" [2002] The Little Magazine: Listen 9.

Senden L, “SOFT LAW, SELF-REGULATION AND CO-REGULATION IN EUROPEAN LAW: Where Do They Meet?” (2005) 9(1) Electronic Journal of Comparative Law.

Shackelford J, Russell S, and Haut J, “BOTTOMS UP: A COMPARISON OF "VOLUNTARY" CYBERSECURITY FRAMEWORKS” (2016) 16 45.

Shackelford S, “Human Rights and Cybersecurity Due Diligence: A Comparative Study” [2017] (50.4) University of Michigan Journal of Law Reform 859 ⟨https://repository.law.umich.edu/mjlr/vol50/iss4/1/⟩.

Shelton D, “Hierarchy of Norms and Human Rights: Of Trumps and Winners” (2002) 65(2) Sasktchewan Law Review.

Siatitsa I, “Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications” (2020) 102(913) International Review of the Red Cross 181 ⟨https://www.cambridge.org/core/product/identifier/S1816383121000047/type/journal_article⟩ accessed 3 March 2024.

Sinha A and others, “From physical security to cybersecurity” [2015] Journal of Cybersecurity tyv007 ⟨https://academic.oup.com/cybersecurity/article-lookup/doi/10.1093/cybsec/tyv007⟩.

Sjøberg J, “European Convention of Human Rights and the Protection of Private Life, Freedom of Expression and Access to Information in a Digital Age” (PhD thesis, Arcada University of Applied Sciences 2023).

Slotwiner DJ and others, “Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians—Proceedings of the Heart Rhythm Society’s Leadership Summit” (2018) 15(7) Heart Rhythm e61 (Publisher: Elsevier Inc.) ⟨https://doi.org/10.1016/j.hrthm.2018.05.001⟩.

Solove DJ, *Nothing to hide: The false tradeoff between privacy and security* (ISSN: 0009-4978 Publication Title: Yale University Press, 2011).

Spurgeon WA and Fagan TP, “Criminal Liability for Life-Endangering Corporate Conduct” (1981) 72(2) Journal of Criminal Law and Criminology 35.

Steinkeller P, “The Renting of Fields in Early Mesopotamia and the Development of the Concept of" Interest" in Sumerian” (1981) 24(2) Journal of the Economic and Social History of the Orient.

Stevens DJ and others, “Obesity surgery smartphone apps: A review” (2014) 24(1) Obesity Surgery 32.

Stoddart K, “Live Free or Die Hard: U.S.-UK Cybersecurity Policies” (2016) 131(4) Political Science Quarterly 803 ⟨https://onlinelibrary.wiley.com/doi/10.1002/polq.12535⟩.

Stoycheff E, Burgess S, and Martucci MC, “Online censorship and digital surveillance: the relationship between suppression technologies and democratization across countries” (2020) 23(4) Information Communication and Society 474 (Publisher: Taylor & Francis) ⟨https://doi.org/10.1080/1369118X.2018.1518472⟩.

Stoykova R, “Encrochat: The hacker with a warrant and fair trials?” (2023) 46 Forensic Science International: Digital Investigation 301602 ⟨https://linkinghub.elsevier.com/retrieve/pii/S2666281723001142⟩ accessed 26 July 2023.

Struppek L and others, “Learning to Break Deep Perceptual Hashing: The Use Case NeuralHash” (_eprint: 2111.06628, 2021) ⟨https://arxiv.org/abs/2111.06628v1⟩.

Stylianou K and Iacovides M, “The goals of EU competition law: a comprehensive empirical investigation” [2022] Legal Studies 1 ⟨https://www.cambridge.org/core/product/identifier/S0261387522000083/type/journal_article⟩.

Subramanian N and others, “Image Steganography: A Review of the Recent Advances” (2021) 9 IEEE Access 23409 (ISBN: 0113180276).

Sullivan J and Deese B, *Executive Order on America’s Supply Chains: A Year of Action and Progresss* (techspace rep, White House 2022) ⟨https://www.whitehouse.gov/wp-content/uploads/2022/02/Capstone-Report-Biden.pdf⟩.

Suryotrisongko H and Musashi Y, "Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective" (IEEE November 2019).

Svenaeus F, *The Hermeneutics of Medicine and the Phenomenology of Health: Steps Towards a Philosophy of Medical Practice* (2nd, The International Library of Bioethics, vol 97, Springer International Publishing 2022) ⟨https://link.springer.com/10.1007/978-3-031-07281-9⟩ accessed 11 July 2023.

Svilicic B and others, "Paperless ship navigation: cyber security weaknesses" (2020) 13(3-4) Journal of Transportation Security 203 ⟨https://link.springer.com/10.1007/s12198-020-00222-2⟩.

T M and others, "Orphan Medical Devices and Pediatric Cardiology – What Interventionists in Europe Need to Know, and What Needs to be Done" (2023) 44(2) Pediatric Cardiology 271 ⟨https://link.springer.com/10.1007/s00246-022-03029-1⟩ accessed 10 October 2023.

Taddeo M, "Is Cybersecurity a Public Good?" (2019) 29(3) Minds and Machines 349 (ISBN: 1102301909507 Publisher: Springer Netherlands) ⟨https://doi.org/10.1007/s11023-019-09507-5⟩.

Tahvanainen A, "Hierarchy of Norms in International and Human Rights Law" (2006) 24(03) Nordic Journal of Human Rights 191 ⟨https://www.idunn.no/ntmr/2006/03/hierarchy_of_norms_in_international_and_human_rights_law⟩.

Tang A and others, "What makes software design effective?" (2010) 31(6) Design Studies 614 (Publisher: Elsevier Ltd) ⟨http://dx.doi.org/10.1016/j.destud.2010.09.004⟩.

Tangney JD, *History of Protection in Computer Systems:* (techspace rep, Defense Technical Information Center 1980) ⟨http://www.dtic.mil/docs/citations/ADA108830⟩.

Taylor L and others, *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020).

TeBrake WHH, "Taming the Waterwolf: Hydraulic Engineering and Water Management in the Netherlands During the Middle Ages" (2002) 43(3) Technology and Culture 475 ⟨http://muse.jhu.edu/content/crossref/journals/technology_and_culture/v043/43.3tebrake.html⟩.

Tolofari SR, Button KJ, and Pitfield DE, "Shipping Costs and the Controversy Over Open Registry" (1986) 34(4) The Journal of Industrial Economics 409 ⟨https://www.jstor.org/stable/2098626?origin=crossref⟩.

Tomsett R and others, "Why the Failure? How Adversarial Examples Can Provide Insights for Interpretable Machine Learning" [2018] 2018 21st International Conference on Information Fusion, FUSION 2018 838 (ISBN: 9780996452762).

Treiman I, "Escaping the Creditor in the Middle Ages" (1927) 43(2) Law Quarterly Review 230.

Trengove M and others, "A critical review of the Online Safety Bill" (2022) 3(8) Patterns 100544 ⟨https://linkinghub.elsevier.com/retrieve/pii/S2666389922001477⟩ accessed 27 September 2023.

Tucker G, "Sustainable Product Lifecycle Management, Industrial Big Data, and Internet of Things Sensing Networks in Cyber-Physical System-based Smart Factories" (2021) 6(1) Journal of Self-Governance and Management Economics 9 ⟨https://addletonacademicpublishers.com/contents-jsme/2091-volume-9-1-2021/3944-sustainable-product-lifecycle-management-industrial-big-data-and-internet-of-things-sensing-networks-in-cyber-physical-system-based-smart-factories⟩.

Tulkens F, "Judicial Activism v Judicial Restraint: Practical Experience of This (False) Dilemma at the European Court of Human Rights" (2022) 3(3) European Convention on Human Rights Law Review 293 ⟨https://brill.com/view/journals/eclr/3/3/article-p293_002.xml⟩ accessed 28 September 2023.

Twining W, "The Bad Man Revisited" [1972] Cornell Law Review 39 ⟨https://www.taylorfrancis.com/books/9781351543767/chapters/10.4324/9781315086323-3⟩.

Umpleby SA, "A Short History of Cybernetics in the United States" (2008) 19(4) Österreichische zeitschrift für geschichtswissenschaften 28.

Unger RW, “Channelling violence at sea: States, international trade and the transformation of naval forces from the high Middle Ages to the age of steam” (2019) 31(2) International Journal of Maritime History 202 ⟨http://journals.sagepub.com/doi/10.1177/0843871419844875⟩.

Ussing H, “The Scandinavian Law of Torts: Impact of Insurance on Tort Law” (1952) 1(4) The American Journal of Comparative Law 359 ⟨https://academic.oup.com/ajcl/article-lookup/doi/10.2307/837349⟩.

Van Blerk N, “The Ancient Egyptians’ “Religious World”: The Foundation of Egyptian Law” (2019) 28(1) Journal for Semitics ⟨https://www.upjournals.co.za/index.php/JSEM/article/view/4389⟩.

Van Daalen OL, “The right to encryption: Privacy as preventing unlawful access” (2023) 49 Computer Law & Security Review 105804 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364923000146⟩ accessed 28 September 2023.

Van den Besselaar P and Gaston H, “Disciplinary, multidisciplinary, interdisciplinary: Concepts and indicators” [2001] ISSI.

Van Der Sloot B, “A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle” (2018) 34(3) Computer Law & Security Review 539 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364917303849⟩ accessed 28 September 2023.

Vandezande N, “Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor” (2024) 52 Computer Law & Security Review 105890 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364923001000⟩ accessed 24 May 2024.

Vasic M and Billard A, “Safety Issues in Human-Robot Interactions” (2013).

VerSteeg R, “Law in Ancient Egyptian Fiction” (1994) 24(1) Georgia Journal of International and Comparative Law 63.

Voas J, Kshetri N, and DeFranco JF, “Scarcity and Global Insecurity: The Semiconductor Shortage” (2021) 23(5) IT Professional 78 ⟨https://ieeexplore.ieee.org/document/9568259/⟩.

Voeten E, “The impartiality of international judges: Evidence from the European court of human rights” (2008) 102(4) American Political Science Review 417.

Wachter S, Mittelstadt B, and Russell C, “Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI” (2021) 41 Computer Law & Security Review 105567 ⟨https://linkinghub.elsevier.com/retrieve/pii/S0267364921000406⟩ accessed 28 September 2023.

Wagner B, “The Politics of Internet Filtering: The United Kingdom and Germany in a Comparative Perspective” (2014) 34(1) Politics 58.

Wakefield JC, “False positives in psychiatric diagnosis: implications for human freedom” (2010) 31(1) Theoretical Medicine and Bioethics 5 ⟨http://link.springer.com/10.1007/s11017-010-9132-2⟩.

Walker CH, “Document Security in the Ancient World” in *Encyclopedia of Information Ethics and Security* (2007).

Wang S and others, “Insecurity of operational cellular IoT service: new vulnerabilities, attacks, and countermeasures” (ACM October 2021) ⟨https://dl.acm.org/doi/10.1145/3447993.3483239⟩.

Ware WH, “Security and privacy in computer systems” [1967] Proceedings of the April 18-20, 1967, Spring Joint Computer Conference 4.

Weiner M and others, “Security analysis of a widely deployed locking system” [2013] Proceedings of the ACM Conference on Computer and Communications Security 929 (ISBN: 9781450324779).

Wellman C, “The Universality and Justification of Human Rights” (2011) 30(3) Criminal Justice Ethics 288.

Westen P, “Two Rules of Legality in Criminal Law” (2006) 26(3) Law and Philosophy 229 ⟨http://link.springer.com/10.1007/s10982-006-0007-7⟩.

White L and Van Basshuysen P, "Without a trace: Why did corona apps fail?" (2021) 47(12) Journal of Medical Ethics E83.

Wirth A, "The economics of cybersecurity" (2017) 51(Horizons) Biomedical Instrumentation and Technology 52.

Wood RG, Understanding Colombia's False Positives (Oxford Transitional Justice Research Working Paper Series 2009).

Wright JF, "Risk management; a behavioural perspective" (2018) 21(6) Journal of Risk Research 710 (Publisher: Routledge) ⟨http://dx.doi.org/10.1080/13669877.2016.1235605⟩.

Wright Q, "Inferences of Science and Technology for International Law" (1955) 4(2) Journal of Public Law 358.

Wu X and Shah Jillani AH, "Admissibility of Lis Pendens in International Commercial Arbitration: A Comparative Insight of Different Legal Systems" (2020) 13(4) Journal of Politics and Law 134.

Xenofontos C and others, "Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies" (2022) 9(1) IEEE Internet of Things Journal 199 ⟨https://ieeexplore.ieee.org/document/9430606/⟩ accessed 28 July 2023.

Yekutieli Y, "Is somebody watching you? Ancient surveillance systems in the southern Judean desert" (2006) 19(1) Journal of Mediterranean Archaeology 65.

Yousefnezhad N, Malhi A, and Främling K, "Security in product lifecycle of IoT devices: A survey" (2020) 171 Journal of Network and Computer Applications 102779 ⟨https://linkinghub.elsevier.com/retrieve/pii/S1084804520302538⟩.

Zannoni D, "GPS Surveillance from the Perspective of the European Convention on Human Rights" (2018) 8(2) European Criminal Law Review 294 ⟨https://www.nomos-elibrary.de/index.php?doi=10.5771/2193-5505-2018-2-294⟩ accessed 28 September 2023.

Zdzikot T, "Cyberspace and Cybersecurity" in *Cybersecurity in Poland* (2022).

Zeng X and others, "Adversarial attacks beyond the image space" (2019) 2019-June Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition 4297 (ISBN: 9781728132938 _eprint: 1711.07183).

Zheng K and Albert LA, "A Robust Approach for Mitigating Risks in Cyber Supply Chains" (2019) 39(9) Risk Analysis 2076 ⟨https://onlinelibrary.wiley.com/doi/10.1111/risa.13269⟩.

— "Interdiction models for delaying adversarial attacks against critical information technology infrastructure" (2019) 66(5) Naval Research Logistics (NRL) 411 ⟨https://onlinelibrary.wiley.com/doi/10.1002/nav.21859⟩.

Zhou ZZ and Choudhary V, "Impact of Competition from Open Source Software on Proprietary Software" (2022) 31(2) Production and Operations Management 731 ⟨https://onlinelibrary.wiley.com/doi/10.1111/poms.13575⟩.

Zuiderveen Borgesius FJ and Steenbruggen W, "The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust" (2019) 20(1) Theoretical Inquiries in Law 291 ⟨https://www.degruyter.com/document/doi/10.1515/til-2019-0010/html⟩ accessed 3 March 2024.

Zweigert K and Kötz H, *An Introduction to Comparative Law* (Third Edition, Oxford University Press 2011).