EJLT European Journal of Law and Technology

The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things

Mattis van 't Schip*

Abstract

An increasing number of actors design, develop and produce modern ICT products in a collaborative network: a supply chain. From a cybersecurity perspective, each actor brings new vulnerabilities for the entire chain and, in turn, the ICT product created by the chain. This problem should be addressed by supply chain cybersecurity, a type of cybersecurity policy that aims to prevent disruption of a supply chain's digital assets by internal or external actors. The EU Network and Information Systems (NIS2) Directive, which was adopted in 2023, introduces rules on supply chain cybersecurity for the network and information systems (e.g., Internet of Things devices) of entities in critical sectors (e.g., energy providers, hospitals). This article shows that the NIS2 Directive aligns closely with established risk management guidelines. Thus, the Directive, at first glance, offers a proper response to supply chain cybersecurity problems. However, the supply chain cybersecurity provisions are a missed opportunity: the provisions build on a flawed and limited understanding of the intricacies of supply chain cybersecurity in practice.

Keywords: supply chain cybersecurity, NIS2 Directive, Internet of Things, data protection.

* Ph.D. Candidate at the Interdisciplinary Research Hub on Digitalization and Society (iHub), Radboud University. This research is funded through the NWO INTERSCT project [NWA.1160.18.301].

1. Introduction

The proliferation of Internet of Things (IoT) devices in industry and everyday life gives rise to new security threats. IoT devices incorporate hardware and software elements; a 'smart' watch can indicate the current time, like a traditional watch, and can send and receive text messages. Attackers increasingly focus on IoT devices as entry points, as their network connection allows for easy access to other resources and devices within the network.[1] IoT devices often operate with constrained functionalities and resources, as manufacturers aim to continuously bring new products to the market.[2] As a result, devices become vulnerable; producers do not make significant security investments for each device and software may not be kept up to date.[3]

In recent years, attackers have shifted their focus to attacks on supply chains, with specific attention to insecure IoT devices. A supply chain is a collaborative network of actors that, together, create, design and develop products and services for consumers.[4] Attackers exploit vulnerabilities in the systems of one actor to subsequently attack a second, main target in the same supply chain.[5] For instance, in the SolarWinds attack, attackers infiltrated a piece of software used by multinational companies for network management.[6] The attackers used this initial infiltration to access systems of SolarWinds users and install malware; an estimated 18,000 SolarWinds costumers installed the malware update, including the United States Department of Homeland Security and Microsoft.[7]

Supply chain attacks and IoT devices are closely linked.[8] Many organisations employ IoT devices to transmit, record and exchange data between supply chain partners; the IoT is thus an important driver of modern supply chains.[9]

---

[1] European Union Agency for Cybersecurity, *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures* (European Network and Information Security Agency 2017).

[2] Sunil Cheruvu et al., *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment* (Apress 2020) 10–12.

[3] European Union Agency for Cybersecurity (n 1) 22–23.

[4] See more extensively John T Mentzer et al., 'Defining Supply Chain Management' (2001) 22 *Journal of Business Logistics* 1, 4.

[5] European Union Agency for Cybersecurity and A Malatras et al. (eds), *ENISA Threat Landscape for Supply Chain Attacks* (European Network and Information Security Agency 2021).

[6] Saheed Oladimeji and Sean Michael Kerner, 'SolarWinds Hack Explained: Everything You Need to Know' (*TechTarget*, 29 June 2022) <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know> accessed 17 January 2024.

[7] ibid.

[8] European Union Agency for Cybersecurity et al., *Guidelines for Securing the Internet of Things – Secure Supply Chain for IoT* (European Network and Information Security Agency 2020); Sandor Boyson, Thomas M Corsi and John-Patrick Paraskevas, 'Defending Digital Supply Chains: Evidence from a Decade-Long Research Program' (2022) 118 *Technovation* 102380; Tope Omitola and Gary Wills, 'Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain' (2018) 126 *Procedia Computer Science* 441.

[9] Martin Serror et al., 'Challenges and Opportunities in Securing the Industrial Internet of Things' (2021) 17 *IEEE Transactions on Industrial Informatics* 2985.

At the same time, the supply chain of IoT devices regularly includes hundreds of actors,[10] which means the chain has a broad and diverse attack surface.[11] A single weak link in this surface can be sufficient for an attack on the supply chain that produces IoT devices. Recently, for instance, threat actors attacked Indian critical infrastructure multiple times, including an attack on the largest Indian power company.[12] Microsoft found that the infrastructure providers used IoT devices which operated on a web server called Boa.[13] The maintainers of this web server discontinued the project in 2005; the web server, today, contains various critical vulnerabilities which threat actors could exploit. The IoT is thus also a major target of supply chain attacks.

As a response to supply chain attacks, organisations now develop supply chain cybersecurity strategies. Supply chain cybersecurity aims to prevent disruption of a supply chain's digital assets by internal or external actors.[14] Until recently, EU cybersecurity legislation did not explicitly require organisations to adopt supply chain cybersecurity measures or policies.[15]

In January 2023, a revision for the EU Network and Information Security (NIS) Directive of 2016, the NIS2 Directive, came in effect.[16] The Directive aims to harmonise cybersecurity across critical sectors in the EU. Therefore, the NIS2 Directive introduces a cybersecurity risk management framework which includes supply chain cybersecurity rules. These rules primarily address entities in critical sectors (e.g., hospitals, energy providers) that employ network and information systems, including

[10] '2021 Apple Supplier List' (2020) <https://www.apple.com/supplier-responsibility/pdf/Apple-Supplier-List.pdf> accessed 13 June 2023.

[11] European Union Agency for Cybersecurity (n 1) 22–23.

[12] Ax Sharma, 'Hive Claims Ransomware Attack on Tata Power, Begins Leaking Data' (*BleepingComputer*, 25 October 2022) <https://www.bleepingcomputer.com/news/security/hive-claims-ransomware-attack-on-tata-power-begins-leaking-data/> accessed 18 January 2024.

[13] Adam Castleman et al., 'Vulnerable SDK Components Lead to Supply Chain Risks in IoT and OT Environments' (*Microsoft Security Blog*, 22 November 2022) <https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/> accessed 18 January 2024.

[14] Myles D Garvey, Jim Samuel and Andrey Kretinin, 'An Ontology of Supply Chain Cybersecurity' in Steven Carnovale and Sengun Yeniyurt (eds), *Cyber security and supply chain management: risks, challenges and solutions* (World Scientific 2021) 106.

[15] The cybersecurity legislation of some Member States did already include supply chain security; see 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 *International Cybersecurity Law Review* 163; Kaspar Rosager Ludvigsen, Shishir Nagaraja and Angela Daly, 'Preventing or Mitigating Adversarial Supply Chain Attacks: A Legal Analysis' Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (ACM 2022).

[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 (NIS2) [2022] OJ L333/80.

IoT devices (e.g., smart watches for patients). Therefore, the NIS2 Directive aims to mitigate supply chain attacks on systems used within critical sectors.

This article answers the following question: to what extent can the NIS2 supply chain cybersecurity rules help mitigate the emergence of supply chain cybersecurity problems for IoT devices used in critical sectors? I argue that, at first glance, the NIS2 supply chain cybersecurity rules can indeed support the current regulatory landscape, as the Directive introduces a set of rules that cover a currently unregulated area of cybersecurity through a suitable risk-based approach. However, the logic of the supply chain cybersecurity measures in the NIS2 Directive is flawed. The Directive does not clearly define integral elements of supply chain cybersecurity, such as the role of the focal company, the governing company within a supply chain. The chosen approach might, therefore, not achieve the aim of mitigating supply chain cybersecurity problems.

This article proceeds as follows. In Section 2, I draw on existing literature in the field of supply chain risk management to indicate how current research frameworks rely on risk management concepts such as cyber resilience, cybersecurity investments, and standardisation to define supply chain cybersecurity. In Section 3, I set out the NIS2 Directive's scope and supply chain cybersecurity provisions. I compare these provisions to the limited role of supply chain cybersecurity in other EU cybersecurity legislation. In Section 4, I analyse the relevance of the NIS2 supply chain cybersecurity approach for the cybersecurity of IoT devices, based on the research frameworks analysed in Section 2. In Section 5, I examine how, regardless of its benefits, the NIS2 Directive cannot offer an effective legal avenue for supply chain cybersecurity rules, as evident by its absence of clear definitions and diffused allocation of responsibilities. Section 6 concludes.

2. Supply Chain Cybersecurity

Modern products consist of hundreds of software and hardware components. Software components have the most significant share in product supply chains; a single software package can integrate numerous other packages (e.g., open-source software). The software supply chain therefore consists of thousands of software components.

IoT devices are primary examples of modern ICT products with diverse software and hardware supply chains. A smart watch combines a traditional physical watch with a software operating system. Both the physical watch and the operating system rely on their own separate components to function (i.e., the battery and software packages respectively).[17] The production process of a smart watch, therefore, consists of various manufacturers, software developers and component suppliers. This network of different co-operating actors expands the cyberattack surface of the smart watch;

[17] 'Apple Watch Teardown' (*iFixit*, 23 April 2015) <https://www.ifixit.com/Teardown/Apple+Watch+Teardown/40655> accessed 18 January 2024.

each actor brings their own IT systems, processes and employees. For each of these domains, cybersecurity vulnerabilities can exist, and threat actors can exploit those vulnerabilities to infiltrate the network.[18] As a result, the cybersecurity of 'supply chains' − the network of actors and processes involved in the creation of a product − is receiving increasing attention.

In this section, I highlight how researchers in risk management studies are developing theories to operationalise supply chain cybersecurity. First, I examine the actors involved in modern supply chains. Second, I analyse the field of supply chain cybersecurity to find its most important characteristics, which I mainly derive from literature in the emerging field of cyber supply chain risk management.

2.1 The Multi-Tiered Supply Chain

The supply chain of an IoT device consists of 'the actors, processes and assets that participate in the realisation (e.g., development, design, maintenance, patch management) of any IoT device.'[19] Within this network of various actors, the focal company has a prominent role. Focal companies 'usually (1) rule or govern the supply chain, (2) provide the direct contact to the customer, and (3) design the product or service offered.'[20] Apple, for instance, is the focal company in the supply chains for Apple Watches. The focal company carries the primary responsibility for the functioning of the supply chain. Focal companies thus also often govern and implement cybersecurity measures for the supply chain.

A supply chain consists of multiple tiers of suppliers that co-operate with the focal company. First-tier suppliers work directly with the focal company and are familiar to them. First-tier suppliers produce direct components for the devices, such as network chips, cameras and batteries, or develop main software operating systems and applications. In certain cases, first-tier suppliers assemble components into a final product for the focal company.

First-tier suppliers integrate components from lower-tier suppliers (e.g., a software component). Lower-tier suppliers co-operate with the tiers above them (e.g., a second-tier supplier with a first-tier supplier) and have an indirect relation with the focal company. Focal companies often struggle with governing those lower-tier suppliers due to the number of suppliers within all tiers of the supply chain.[21] The focal company might, for instance, struggle with assessing the risks of cybersecurity

[18] Hugh Boyes, 'Cybersecurity and Cyber-Resilient Supply Chains' (2015) *Technology Innovation Management Review* 7.
[19] European Union Agency for Cybersecurity (n 8) 9.
[20] Stefan Seuring and Martin Müller, 'From a Literature Review to a Conceptual Framework for Sustainable Supply Chain Management' (2008) 16 *Journal of Cleaner Production* 1699, 1699.
[21] Liyuan Wang-Mlynek and Kai Foerstl, 'Barriers to Multi-Tier Supply Chain Risk Management' (2020) 31 *The International Journal of Logistics Management* 465.

incidents at lower-tier suppliers (e.g., vulnerabilities in components).[22] Multi-tier supply chain management, the governance of all tiers of the supply chain, is thus an important task of the focal company.

The supply chain also includes the importer, distributor and the seller. They are the entities that ensure the product reaches the consumer. Often, factories worldwide create IoT devices, which means importers must bring the product to the EU market. The distributor transports the product to stores in the Union, where sellers offer the product to the consumer.

Figure 1: Multi-Tier Supply Chain

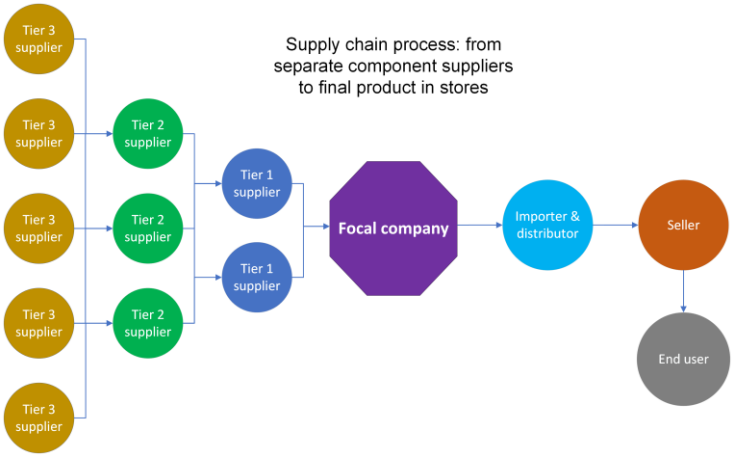


Figure 1 1 illustrates a multi-tier software and hardware supply chain. Apple's smart watch exemplifies this multi-tier supply chain well. Apple is the focal company that manages the supply chain and ensures that the development process runs smoothly. Foxconn, a Chinese company, manufactures the smart watches;[23] Foxconn is a prominent tier 1 supplier of Apple products.[24] Apple, through Foxconn, has multiple lower-tier suppliers (e.g., camera suppliers, battery suppliers). Together with the hardware supply chain, software suppliers ensure that the smart watch integrates an operating system with different functioning applications. After assembly, the watches

[22] Jason K Deane et al., 'Managing Supply Chain Risk and Disruption from IT Security Incidents' (2009) 2 *Operations Management Research* 4.
[23] Joe Rossignol, 'Foxconn and Compal Will Reportedly Assemble "Apple Watch Series 6" Models Next Year' (*MacRumors*) <https://www.macrumors.com/2019/10/23/apple-watch-series-6-foxconn-compal/> accessed 18 January 2024.
[24] Jenny Chan, *Dying for an Iphone: Apple, Foxconn, and the Lives of China's Workers* (Haymarket Books 2020).

are exported from China to, for example, the EU, where distributors bring the devices to sellers in stores. The end user, finally, is part of many ICT product supply chains, as they can return the device to the chain, or request maintenance.[25]

2.2 The Developing Field of Supply Chain Cybersecurity

The multi-tiered supply chain highlights the various actors involved in a smart watch's production process. Supply chain cybersecurity measures aim to mitigate the diverse cybersecurity threats that each of these actors, with their own people, processes and technologies, can cause.[26]

Research of supply chain cybersecurity remains limited to a few distinct fields, predominantly in risk management studies.[27] As a result of this recent emergence, Garvey et al. found that existing literature on supply chain cybersecurity does not define the concept clearly.[28] In turn, they offer their own definition of supply chain cybersecurity as 'the collection of strategies, policies, and processes that manage and mitigate against the possible loss of cyber assets and the possible subsequent disruption of any supply chain process that manifests as a result of the loss of a cyber asset.'[29]

Under this definition, supply chain cybersecurity requires knowledge of the risks associated with the cyber assets that actors use in the supply chain (e.g., IoT devices). Such risks diverge between software and hardware components. The typical supply chain cybersecurity risk for hardware is hardware tampering (e.g., to create back doors), while for software, the risks mainly lie with software vulnerabilities in the numerous integrated software packages (e.g., as in the SolarWinds attack).[30] Supply chain cybersecurity is therefore a broad topic: many different actors across the supply chain must take cybersecurity measures and, as actors can vary significantly, supply chain cybersecurity covers a broad range of actor-tailored cybersecurity measures.[31]

Current theories on how to operationalise supply chain cybersecurity mainly stem from Cyber Supply Chain Risk Management (CSCRM) studies. This emerging field combines 'approaches, methods and practices from the fields of cybersecurity,

[25] This holistic view of the supply chain is often coined as the 'end-to-end supply chain'. See <https://supplychainmanagement.utk.edu/blog/end-to-end-supply-chain-planning/> accessed 30 January 2024.
[26] European Union Agency for Cybersecurity (n 5).
[27] Arne Roar Nygård and Sokratis Katsikas, 'SoK: Combating Threats in the Digital Supply Chain', Proceedings of the 17th International Conference on Availability, Reliability and Security (ACM 2022).
[28] Garvey, Samuel and Kretinin (n 14).
[29] ibid 106.
[30] Omitola and Wills (n 8).
[31] See, e.g., the issue of sea piracy, which not all actors in the supply chain have to consider; Alexa K Sullivan, 'Piracy in the Horn of Africa and Its Effects on the Global Supply Chain' (2010) 3 *Journal of Transportation Security* 231.

enterprise risk management, and supply chain management.'[32] CSCRM studies examine how organisations develop strategies and policies that prevent and mitigate cybersecurity threats to the supply chain.[33] Overall, three elements are highly prevalent in current CSCRM literature: 1) cyber resilience; 2) the required collaborative cybersecurity investments to achieve that resilience; and 3) the use of recognised standards.[34] These three elements build upon each other: cyber resilience requires appropriate cybersecurity investments, while these investments are most efficient when the actors in the chain collaborate, which standardisation supports.

2.2.1 Cyber Resilience

'Cyber resilience' refers to the capacity of the supply chain to recover after cyberattacks. Cyber resilience is therefore a component of cybersecurity. Without resilience, cyberattacks might interrupt the supply chain's production process longer than necessary. Appropriate cyber resilience strategies ensure that the production processes can continue swiftly after an attack.

Boyes models the cyber resilience capacity of a supply chain along three perspectives: 1) the continuity of operations; 2) the control of access and system operations; 3) the quality and validity of information.[35] Cyber resilience therefore intertwines organisational and technical resilience measures. As Davis notes, cyber resilience 'is a business issue and should be woven into business or enterprise risk management [and] it should be considered across all business operations.'[36] Cyber resilience is thus a combination of different business-specific requirements; a general approach for each supply chain does not exist. Therefore, each actor within the supply chain must examine what improvements they can make for their own organisation.

In supply chain risk management, cyber resilience is separate from cybersecurity.[37] Cyber resilience stems from the belief that insecurity is, as Bygrave notes, 'a basic, inescapable condition of the digital world'.[38] In this context, cybersecurity and cyber resilience differ: cybersecurity strategies aim to prevent incidents, while cyber resilience strategies assume certain cybersecurity incidents are inescapable and, therefore, aim to ensure that services and processes can recover from security

[32] Sandor Boyson, 'Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems' (2014) 34 *Technovation* 342, 342.
[33] ibid.
[34] Steven A Melnyk et al., 'New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain' (2022) 60 *International Journal of Production Research* 162, 172–173.
[35] Boyes (n 18) 30.
[36] Adrian Davis, 'Building Cyber-Resilience into Supply Chains' (2015) *Technology Innovation Management Review* 9, 24.
[37] Fredrik Björck et al., 'Cyber Resilience – Fundamentals for a Definition' in Alvaro Rocha et al. (eds), *New Contributions in Information Systems and Technologies*, vol 353 (Springer International Publishing 2015).
[38] Lee A Bygrave, 'Cyber Resilience versus Cybersecurity as Legal Aspiration', 14th International Conference on Cyber Conflict: Keep Moving! (CyCon) (2022) 29.

incidents. CSCRM theories specifically emphasise the need for cyber resilience to ensure supply chains can continue operations regardless of cyber threats.[39]

However, modern cybersecurity practice does not clearly distinguish between cybersecurity and cyber resilience.[40] European cybersecurity law brings this lack clarity to the fore, as it mainly promotes flexible security strategies (e.g., with 'security-by-design' policies).[41] The transition from cybersecurity in supply chain risk *management* towards supply chain *regulation*, therefore, requires attention to both cybersecurity and cyber resilience. Supply chain cybersecurity in legislation thus usually integrates cyber resilience (as recovery measures) into a broad cybersecurity strategy that involves numerous other security measures (e.g., prevention, detection).

2.2.2 Collaborative Cybersecurity Investments

Creazza et al. refer to the relationship between cybersecurity investments and cyber resilience as 'cyber supply chain balanced resilience': a balanced approach between the cyber risks posed to the particular supply chain and the investments made to prevent those risks from impacting that chain.[42] Cybersecurity investments balance the risk of cybersecurity breaches and its effects on the supply chain against the value of taking increased supply chain cybersecurity measures (e.g., stronger awareness campaigns or adopting new, more secure technologies).[43]

With the balanced approach, managers of companies within the supply chain can invest in cybersecurity relative to the risks posed to their company. Generally, smaller suppliers might *want* to improve their overall cybersecurity, but simply lack the necessary knowledge or resources.[44] Cybersecurity investments therefore rely on the specific organisational capacities of each supply chain member. Larger organisations within the supply chain must thus also consider the risks posed to the network of actors when smaller organisations cannot sufficiently invest in cybersecurity. The focal company, for instance, might offer financial resources or cybersecurity awareness campaigns to smaller organisations. With these joint investments, the

[39] In line with the definition in Björck et al. (n 37) 312.
[40] Bygrave (n 38).
[41] ibid.
[42]; Alessandro Creazza et al., 'Who Cares? Supply Chain Managers' Perceptions Regarding Cyber Supply Chain Risk Management in the Digital Transformation Era' (2022) 27 *Supply Chain Management: An International Journal* 30, 32; Claudia Colicchia, Alessandro Creazza and David A Menachof, 'Managing Cyber and Information Risks in Supply Chains: Insights from an Exploratory Analysis' (2019) 24 *Supply Chain Management: An International Journal* 215, 234.
[43] Tadeusz Sawik, 'Balancing Cybersecurity in a Supply Chain under Direct and Indirect Cyber Risks' (2022) 60 *International Journal of Production Research* 766.
[44] Melnyk et al. (n 34) 173–174; Jillian K Kwong and Keri Pearlson, 'Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs' (Proceedings of the 57th Hawaii International Conference on System Sciences, 2024) <https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/957a908a-cf71-47e7-84ac-ee3a2d8c088c/content> accessed 3 January 2024; Davis (n 36).

entire chain is more secure, instead of merely the actors that possess the financial or organisational means.[45]

Finally, the supply chain profits from a balanced resilience investment approach as the benefits of the investments become more visible. If Supplier A and Supplier B make different cybersecurity investments, the benefits and pitfalls of both strategies are not visible to both suppliers.[46] Furthermore, suppliers cannot see the benefits of their investments for the overall security of the chain, thus reducing incentives to continue investing.[47] A balanced and collaborative approach to cybersecurity investments is therefore crucial in improving the cybersecurity of the supply chain.

2.2.3 Standardisation

'Standardisation' refers to a set of guidelines that offer recommendations or requirements for specific processes, systems, services or products. Standards can support the improvement of the overall security level of the supply chain, by prescribing a framework for harmonisation of security throughout the chain.[48] The focal company can, for instance, mandate suppliers to adhere to certain security standards. Standard-setting bodies (e.g., the ISO) or the focal company can subsequently decide to audit the security of the supply chain according to the requirements of the standards.

However, standardisation comes with some uncertainties. First, many standards remain in development, especially in the field of supply chain cybersecurity.[49] Current standards often focus on individual risks, instead of on the interdependencies between organisations.[50] Before harmonised frameworks are possible, most organisations must wait for the standards to materialise. Second, standards can differ significantly per sector or even per organisation, which might impede efforts for cross-sector issues such as supply chain cybersecurity, which affects a diverse set of sectors.[51] Finally, standards can sometimes give the impression of strong security *on paper*, while not necessarily improving security *in practice*.[52] Proper standardisation is more than just checking certain boxes; instead, it requires the adoption of tangible

[45] Yanhui Li and Lu Xu, 'Cybersecurity Investments in a Two-Echelon Supply Chain with Third-Party Risk Propagation' (2021) 59 *International Journal of Production Research* 1216.
[46] ibid.
[47] Yuhong Li et al., 'Ripple Effect in the Supply Chain Network: Forward and Backward Disruption Propagation, Network Health and Firm Vulnerability' (2021) 291 *European Journal of Operational Research* 1117.
[48] Melnyk et al. (n 34) 173; Davis (n 36).
[49] Abhijeet Ghadge et al., 'Managing Cyber Risk in Supply Chains: A Review and Research Agenda' (2019) 25 *Supply Chain Management: An International Journal* 223; Nygård and Katsikas (n 27).
[50] Stefan Schauer, Nineta Polemi and Haralambos Mouratidis, 'MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology' (2019) 12 *Journal of Transportation Security* 1.
[51] Tania Wallis, Chris Johnson and Mohamed Khamis, 'Interorganizational Cooperation in Supply Chain Cybersecurity: A Cross-Industry Study of the Effectiveness of the UK Implementation of the NIS Directive' (2021) 48 *Information & Security: An International Journal* 36, 53–54.
[52] Kwong and Pearlson (n 44) 6660.

organisational and technical change. Strong supply chain cybersecurity standardisation thus requires development of cross-sector standards that go beyond just ensuring strong security on paper; legislation, such as the NIS2 Directive, can stimulate such development.

In sum, supply chain cybersecurity is a rather novel field of study; at a wide, conceptual level, it requires that a broad set of actors within the supply chain adopt a diverse set of cybersecurity measures.

CSCRM researchers offer more precise guidance on how to implement these conceptual conditions. I examined three prevalent elements of this implementation. First, the supply chain must focus on improving its cyber resilience, as part of a broader cybersecurity strategy. Second, the chain must establish this strategy through appropriate collaborative cybersecurity investments. Third, the use of harmonised standards should support baseline levels of security throughout the chain.

3. The NIS2 Supply Chain Cybersecurity Approach

The Network and Information Security Directive (NIS1) of 2016 was the EU's first fully cybersecurity-focused legislation.[53] The aim of the NIS1 was to enhance cybersecurity across the EU, specifically by ensuring a high level of protection for network and information systems (e.g., IoT devices, communication networks).[54] To achieve this aim, NIS1 had three main tenets: 1) cross-border co-operation between Member States; 2) national cybersecurity strategies; and 3) national supervision of network and information systems used in critical sectors.

The scope of NIS1 covered several critical sectors (e.g., energy providers, hospitals). NIS1 aimed to improve the overall cybersecurity of those sectors, as disruptions in their services could prove especially critical.[55] Therefore, NIS1 obligated Member States to adopt national strategies and measures to improve the security of network and information systems. NIS1 divided entities in two categories: operators of essential services (e.g., electricity providers and hospitals);[56] and digital service providers (online marketplaces, search engines and cloud computing services).[57]

Overall, NIS1 succeeded in making Member States introduce cybersecurity legislation that applied broadly across sectors, which brought more attention to the need for strong cybersecurity in those fields.[58] However, the Commission found that the NIS1 Directive could not fully cope with evolving cybersecurity threats and risks, due to the

[53] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1 (NIS1).
[54] Recitals 1–3 NIS1 and Art. 4(1) NIS1.
[55] Recitals 1–3 NIS1.
[56] Art. 4(4) and Annex II NIS1.
[57] Art. 4(5), (6) and Annex III NIS1.
[58] Wallis, Johnson and Khamis (n 51) 51.

Directive's scope and enforcement mechanisms. These difficulties led to the Commission's NIS2 proposal.[59] NIS1 will be repealed after the transposition deadline of NIS2 in October 2024.[60]

3.1 The Scope of NIS2

NIS2 builds on some elements of NIS1. NIS2 still applies to the cybersecurity of a network and information system used by entities in several critical sectors. The definition of network and information systems does not differ from NIS1. IoT devices and other network and information systems (e.g., laptops) thus remain in scope of NIS2.

The two Directives have the same aim: to protect society from cybersecurity issues in the most critical sectors (e.g., energy, water supply).[61] NIS2 applies to specific 'essential' and 'important entities', which build on the 'operators of essential services' and 'digital service providers' of NIS1 respectively.[62]

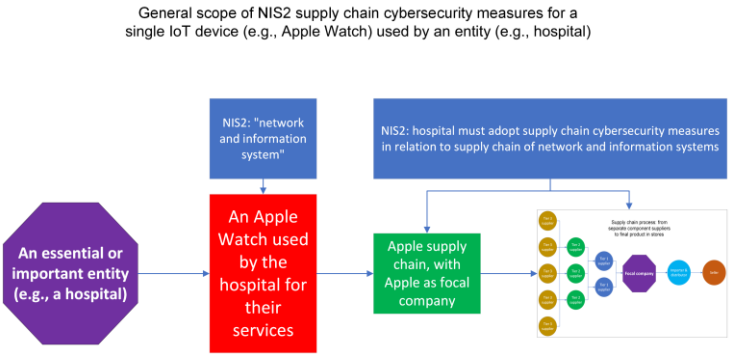
NIS2 broadens the scope of entities from NIS1. Essential entities now include, inter alia, public administration entities.[63] The new category of important entities includes the manufacturing industry, a prominent user of 'Industrial' IoT devices (e.g., network-connected machinery).[64] The Industrial IoT devices exemplify the scope of NIS2: the devices are *network and information systems* that manufacturers, an *important entity*, *use to provide their services*.[65] Figure 2 illustrates this scope in more detail.

The Commission decided to exclude most small and micro-sized enterprises from the scope of NIS2.[66] This is for two reasons. First, the enforcement capabilities of Member States created a major issue in NIS1: Member States were not able to enforce the NIS1 obligations in a coherent manner as their identification of essential entities differed significantly (e.g., the minimum number of customers for water supply operators varied from 10,000 in one Member State to 500,000 in another).[67] If the Commission included small and micro-sized enterprises in the scope of NIS2, Member States would have to identify all relevant enterprises within the sectors of NIS2. This

[59] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM (2020) 823 final (NIS2).
[60] Art. 44 NIS2.
[61] Art. 1(1) and Recital 1 NIS2.
[62] Art. 2 NIS2.
[63] Annex I(10) NIS2.
[64] Annex II(5) NIS2.
[65] See, e.g., the wording of Art 21 NIS2 and Section 3.2 below.
[66] Art. 2(1) NIS2; Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L124/36.
[67] Commission, 'Impact Assessment Report Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148' SWD (2020) 345 final 23.

would create a significant administrative burden for the Member States, which would stand in the way of effective enforcement, according to the Commission.[68] Second, the Commission does not want to burden small and micro-sized enterprises with the significant security investments that compliance with the Directive could require.[69] I address the significance of this exclusion for supply chain cybersecurity in more detail in Section 5.1.

Figure 2: NIS2 General Scope for Supply Chain Cybersecurity Provisions



3.2 Supply Chain Cybersecurity Provisions

NIS2 contains several obligations for the cybersecurity of supply chains. Two main actors are involved in these obligations: the Member States and the essential and important entities (henceforth 'IoT-using entities'). The obligations do not explicitly address focal companies or suppliers.[70] NIS2 came in effect at the same time as the Digital Operational Resilience Act (DORA), which introduced similar rules – including supply chain cybersecurity rules – for financial institutions.[71]

[68] ibid 74.
[69] ibid 73.
[70] The focal company is addressed indirectly if it also manufactures its products. However, this condition does not apply to all focal companies, which means that only specific focal companies are indirectly addressed (as manufacturing IoT-using entities) by the provisions. The notion of a focal company, separately, does not exist in NIS2. See further Section 5.2.
[71] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L333/1. The DORA is a *lex specialis* for the banking sector, while NIS2 is a *lex generalis*. This article therefore focuses on NIS2.

Member States have a prominent role in guiding supply chain cybersecurity. First, they must adopt national policies which address supply chain cybersecurity (Article 7). Second, Member States must ensure that IoT-using entities adopt a cybersecurity risk management strategy, which includes supply chain cybersecurity measures (Article 21). Third, as part of a wider Coordination Group, together with the European Union Agency for Cybersecurity (ENISA) and the Commission, Member States must conduct risk assessments of the supply chains of particularly critical products used by IoT-using entities (Article 22).

Article 7(2)(a) requires Member States to adopt national policies that address the cybersecurity of supply chains. Since NIS1, all Member States have adopted such national cybersecurity strategies.[72] However, many of these strategies do not yet consider supply chain cybersecurity.[73] Pursuant to Article 7(2)(a), Member States must now state in their strategies how they will enhance supply chain cybersecurity for devices employed by essential and important entities. The exact policies might thus differ per Member State.

Article 21 prescribes a cybersecurity risk management approach for IoT-using entities. The entities must take appropriate and proportionate technical and organisational measures to manage supply chain risks. IoT-using entities must take the supply chain cybersecurity measures as part of an 'all-hazard approach', which requires attention to both technological (e.g., unauthorised access) and physical (e.g., theft and fire) environments.[74] Pursuant to Article 21, IoT-using entities must, as part of a broader supply chain cybersecurity strategy, assess the vulnerabilities of each of their *direct* suppliers or service providers.[75] The Directive does not explicitly identify which suppliers are understood as the direct suppliers of an IoT-using entity.

The IoT-using entities must conduct the supply chain risk assessment on the basis of the 'overall quality of products and cybersecurity practices of their suppliers and service providers'.[76] Therefore, the entities cannot rely on generic risk assessments for the supply chains of the devices that they use; they must continuously adapt to the characteristics and risks of the particular supply chain. The essential and important entities (e.g., a hospital that uses medical IoT devices) must thus collaborate intensively with IoT-producing focal companies (e.g., a multinational such

[72] See for an overview of national security strategies: European Union Agency for Cybersecurity, 'National Cyber Security Strategies – Interactive Map' <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map> accessed 30 January 2024.
[73] Germany has a substantial cybersecurity strategy, which also includes some references to supply chain cybersecurity; see Cyber Security Strategy for Germany 2021. Based on a quick survey, the term 'supply chain' (or 'chain') is not found in many other national strategies yet.
[74] Recital 79 NIS2.
[75] The European co-legislators added the condition for a direct relation; it did not exist in the initial Commission proposal.
[76] Art. 21(3) NIS2.

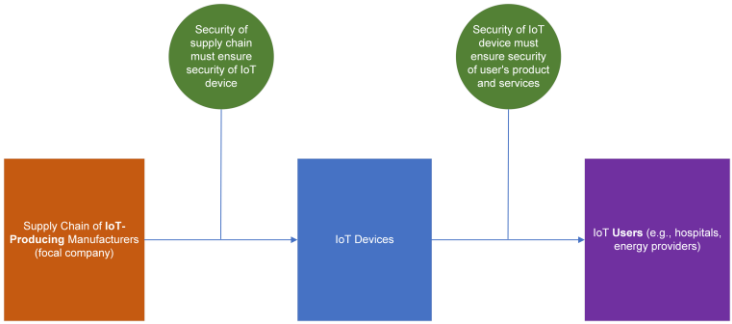
as Philips) and other direct suppliers. In Section 5.2, I analyse whether Article 21's allocation of responsibilities is effective.

To support IoT-using entities in taking appropriate measures, Article 21 requires the entities to take into account European or internationally accepted standards relevant to the security of network and information systems (e.g., ISO standards). As illustrated earlier, such standards could theoretically contribute to harmonised supply chain cybersecurity measures throughout the IoT-producing chain, as each actor takes similar cybersecurity measures. The standards can thus support the collaboration Article 21(2)(d) requires.

Finally, Article 22(1) includes the option for co-ordinated risk assessments of supply chains. The Cooperation Group, which is composed of representatives of ENISA, the Commission and Member States,[77] can carry out assessments of critical ICT products and services for supply chains, based on technical and non-technical risk factors.[78] The Group can rely on several criteria in its decision to perform a risk assessment, including the importance of the ICT product for essential and important entities, the critical functions of the product, and the resilience of the overall supply chain against disruptive events.[79]

The Directive requires supply chain cybersecurity measures from IoT-using entities with methods that strongly resemble cyber supply chain risk management. Figure 3 illustrates this framework. I will address the benefits of this approach for IoT cybersecurity in Section 4.

Figure 3: The Supply Chain Cybersecurity Process in the NIS2 Directive



[77] Art. 14(3) NIS2.
[78] Art. 22(1) NIS2.
[79] Recital 91 NIS2.

3.3 The Novelty of Supply Chain Cybersecurity Regulation

Supply chain cybersecurity rules did not exist in legislation prior to NIS2 and the Digital Operational Resilience Act. In this section, I briefly highlight how these supply chain rules differ from security rules in existing (the General Data Protection Regulation) and forthcoming legislation (the Cyber Resilience Act).[80] I identify how the security provisions in this legislation differ from supply chain cybersecurity provisions, based on the two preconditions of supply chain cybersecurity from Section 2.2: rules must cover: 1) a variety of actors within the supply chain; and 2) a diverse set of cybersecurity measures, to ensure that actors take measures tailored to their organisation.

3.3.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) contains rules for the processing of personal data. In that context, the GDPR prescribes several cybersecurity requirements.

From a supply chain perspective, the main rule that emerges in the GDPR is the security of processing between the *controller* and the *processor*.[81] The controller determines the means and purposes of personal data processing (e.g., Apple for their digital watches), while the processor is an actor employed *by the controller* for data processing (e.g., a cloud service).[82] The controller and processor must securely process personal data, for example through the use of encryption measures.[83]

The GDPR also includes an option for further 'sub-processors' hired by the initial processor, which means it allows for a layered chain of multiple data-processing actors.[84] In the supply chain context, this chain resembles the relationship between focal companies – the 'controllers' of the supply chain – and their multi-tiered suppliers. Therefore, the GDPR acknowledges the importance of cybersecurity rules that apply to different partners in a data processing activity.

At the same time, the GDPR has a limited approach, as it only applies to the actors that *process personal data*. These actors have suppliers (e.g., hardware component suppliers) that do not process personal data. The GDPR does not apply to those actors, even though they play a key role for the security of the personal data.[85]

---

[80] For a broader overview of the IoT cybersecurity regulatory landscape, see Pier Giorgio Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' (2022) *International Review of Law, Computers & Technology* 1.
[81] Art. 32 GDPR.
[82] Art. 4(7), (8) GDPR.
[83] Art. 32 GDPR.
[84] Art. 28(4) GDPR.
[85] PTJ Wolters, 'The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?' (2017) 7 *International Data Privacy Law* 165.

3.3.2 Cyber Resilience Act

The European Commission proposed the Cyber Resilience Act (CRA) in September 2022,[86] with the aim of introducing a comprehensive cybersecurity framework for 'products with digital elements', i.e., any software or hardware product.[87] The most recent version of the CRA is the compromise text of the Council and Parliament from December 2023.[88]

The CRA is not the first product regulation to bring security requirements for the IoT. The Radio Equipment Directive (RED) applies to manufacturers, importers and distributors of radio equipment that is brought to the EU market.[89] In a Delegated Regulation, the Commission determined that IoT devices are a specific category of radio equipment that must comply with certain requirements of the Directive.[90] The Directive requires IoT devices to contain security measures that prevent the device from harming its network resources or from violating the privacy and data protection of the end user.[91] The CRA builds on RED's security requirements and extends them to several different categories.[92]

The CRA applies when a product is brought to the EU market;[93] therefore, manufacturers of products with digital elements are primarily responsible under the Act. The Act defines 'manufacturers' as natural or legal persons who *manufacture* or *develop* software or hardware products.[94] These developers or manufacturers must also market the product under their name or trademark. This 'marketing condition' means that, in supply chain terms, the CRA primarily applies to the focal company, not to all software developers and manufacturers within the supply chain. Importers, distributors and other natural persons have the same obligations as manufacturers when they act as a manufacturer (e.g., by bringing the product to the European market).

---

[86] 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 (CRA).

[87] Art. 3(1) CRA.

[88] Council of the European Union, 'Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 − Letter sent to the European Parliament' [2023] 17000/23. ('CRA' in the footnotes refers to this compromise text.)

[89] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ L153/26 (RED).

[90] Commission Delegated Regulation (EU) 2022/30 of 29.10.2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive [2022] OJ L7/6.

[91] Art. 3(3) RED.

[92] Recital 15 CRA.

[93] Art. 1 CRA.

[94] Art. 3(18) CRA.

Products must comply with a broad set of cybersecurity requirements.[95] Security-by-design is a main component of those requirements; the Act requires that all products ‘shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity’.[96] This security-by-design requirement implicitly covers supply chains, as design, development and production are all part of the supply chain process. However, the more extensive list of cybersecurity requirements in Annex I of the Act lacks an explicit reference to supply chain cybersecurity. The requirements therefore only serve supply chain cybersecurity by independently supporting the overall cybersecurity of software and hardware.[97]

Article 10 lists several separate obligations for manufacturers. One obligation does seem to refer to supply chain cybersecurity, as manufacturers must ‘exercise due diligence when integrating components sourced from third parties in [their products]’.[98] In addition, manufacturers must ensure that the components do not compromise the security of their end product.[99] This obligation requires a certain level of attention to the manufacturer’s supply chain. However, acting with ‘due diligence’ is a rather open-ended obligation. Nonetheless, the Act requires a certain level of attention to secure design, development and integration of components.

3.3.3 Current Legislation in Comparison to NIS2

The NIS2 Directive, when compared to similar legislation, requires more explicit and comprehensive supply chain cybersecurity measures from IoT-using entities. Similar pieces of legislation mainly lack the preconditions of supply chain cybersecurity: their scopes are limited to certain actors within the supply chain and those actors are responsible for certain specific cybersecurity measures. Table 1 summarises these problems for the GDPR and the CRA.[100]

[95] Art. 5(1) and Annex I CRA.
[96] Art. 1(1) Annex I CRA.
[97] Recital 8 CRA.
[98] Art. 10(4) CRA.
[99] ibid.
[100] See also about national legal approaches to supply chain cybersecurity: Ludvigsen, Nagaraja and Daly (n 15).

Table 1: The Lack of Supply Chain Cybersecurity Provisions in Current EU Cybersecurity Legislation

Scope	**GDPR**	**CRA (compromise text)**
Supply chain actors in scope	Processors of personal data (e.g., software developers, cloud providers).	Manufacturers and developers, importers, distributors, other persons acting as manufacturer, when they market the product under their name.
Cybersecurity measures in scope	Only cybersecurity measures required for secure processing of personal data.	Various cybersecurity measures, including security-by-design and secure integration of components. Intended as independent cybersecurity components that support overall supply chain cybersecurity.
Tangible supply chain cybersecurity measures	No, scope of actors and measures restricted to personal data processing.	Scope of actors restricted mainly to focal companies. Security-by-design and secure integration of components indicate growing concern for supply chain cybersecurity at EU level.

NIS2 does regulate supply chain cybersecurity: it covers all *direct* suppliers and service providers of entities, without discerning between the activities of the suppliers. It also requires an all-hazard approach: supply chain cybersecurity is an element of broader cybersecurity risk management.

4. NIS2 Cyber Supply Chain Risk Management

NIS2 approaches supply chain cybersecurity through a risk management lens; some elements of this legal approach therefore coincide with the frameworks developed in CSCRM studies. NIS2, too, integrates efforts to improve cyber resilience with

attention to cyber investments and standardisation. I briefly review below the integration of these three elements to place the NIS2 provisions in a supply chain management context.

4.1 Addressing Cyber Resilience within Cybersecurity

NIS2 requires IoT-using entities to take an all-hazard approach to, inter alia, preventing cyberattacks from impacting their services,[101] employing both technological and physical protection of network and information systems to achieve this.[102]

It also requires IoT-using entities to address cyber resilience within their cybersecurity risk management. The entities must aim to ensure that recipients of their services (e.g., patients in a hospital) do not encounter the effects of a cyberattack.[103] This mitigation of effects is inherent to a cyber resilient organisation: if an attack happens, the organisation must swiftly recover and prevent further problems. In the specific context of supply chain cybersecurity, NIS2 further confirms this aim, stating that IoT-using entities should specifically assess the resilience of products and services of their suppliers.[104] Resilience is also a key element for the risk assessment of critical products by the Coordination Group.[105] Cyber resilience, therefore, has a prominent role in the flexible NIS2 cybersecurity risk management approach.

4.2 Collaborative Cybersecurity Investments

NIS2 aims to incentivise the IoT-using entities to make cybersecurity investments, as it suggests the integration of cybersecurity risk management in the contractual arrangements between the entities and the suppliers of their devices.[106] To comply with these arrangements, IoT-producing actors may need adequate supply chain cybersecurity to continue their product sales.

The actual efficacy of NIS2 on the cybersecurity investments by IoT-producing organisations strongly depends on several conditions. First, as Woods and Ceross highlight, the question remains whether organisations invest to improve their security

---

[101] Art. 21(1) NIS2.

[102] Recital 79 NIS2: 'The cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena.'

[103] Art. 21(1) NIS2: 'entities take […] measures […] to prevent or minimise the impact of incidents on recipients of their services'.

[104] Recital 85 NIS2.

[105] Recital 91 NIS2.

[106] Recital 85 NIS2: 'Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers.' This contract management could even cover other suppliers than the direct supplier, as Recital 85 further states: 'Those entities could consider risks stemming from other levels of suppliers and service providers.'

practices or merely to prevent legal risks associated with non-compliance.[107] Further, the effects of any regulation-induced cybersecurity investment rely on the specific capabilities and security practices of each organisation and their existing resource allocations.[108]

To support proper resource allocation, NIS2 places responsibility for cybersecurity governance with the management bodies of IoT-using entities.[109] Management bodies must, for instance, approve the implementation of the cybersecurity risk framework of Article 21. Article 20(1) also requires Member States to implement provisions that can hold the management bodies liable for infringements of Article 21. In addition, management bodies must follow cybersecurity training, so that they are able to identify and assess cybersecurity risks in their organisation.[110] Given these responsibilities, management bodies are directly involved in cybersecurity risk management and might therefore more quickly acknowledge the necessity of proper cybersecurity investments.[111]

4.3 Standardisation

NIS2 supports the integration of security standards in supply chain management in several ways.

First, Article 21 specifically notes that IoT-using entities must take European and international standards into account as part of their cybersecurity risk management. The supply chain cybersecurity measures should thus, where feasible, stem from European or international security standards.[112]

Second, NIS2 requires the Commission, ENISA and Member States to promote the use of standards.[113] Moreover, this group must take an active role in maintaining relations with standard-setting bodies and in fostering opportunities for future co-operation.[114] Standards are therefore key components of NIS2's cybersecurity framework.

---

[107] Daniel W Woods and Aaron Ceross, 'Blessed Are The Lawyers, For They Shall Inherit Cybersecurity' Proceedings of the 2021 New Security Paradigms Workshop (Association for Computing Machinery 2022).

[108] Lawrence A Gordon et al., 'Increasing Cybersecurity Investments in Private Sector Firms' (2015) *Journal of Cybersecurity* 3.

[109] Art. 20(1) NIS2.

[110] Art. 20(2) NIS2.

[111] Niels Vandezande, 'Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor' (2024) 52 *Computer Law & Security Review* 105890, 7–8.

[112] Art. 21(1) NIS2: 'Taking into account the state-of-the-art and, where applicable, relevant European and international standards, the [security] measures shall ensure a level of security […] appropriate to the risks posed.'

[113] Art. 25(1) and Recital 80 NIS2.

[114] Art. 25 and Recital 59.

5. Supply Chain Cybersecurity beyond NIS2: Perfecting the Approach

The introduction of supply chain cybersecurity regulation in NIS2 offers, at first glance, a proper response to supply chain cybersecurity threats. At the same time, supply chain cybersecurity only has a limited role in NIS2, as a component of a broader risk management approach.

In this section, I highlight two emerging problems from the limited role of supply chain cybersecurity in NIS: first, an overall lack of clear definitions about supply chains and supply chain cybersecurity; second, the focus of NIS2 on the IoT-using entity, instead of the focal company.

As a result of both problems, NIS2 is most beneficial for supply chain cybersecurity if the European legislators utilise it as groundwork for further, concentrated supply chain cybersecurity regulation.

5.1 What is Supply Chain Cybersecurity?

Recent literature reviews indicate an overall lack of clear definitions within the supply chain cybersecurity field.[115] NIS2 suffers from similar problems: it lacks distinct definitions for the 'supply chain' and, as a result, for 'supply chain cybersecurity'. This is surprising, given the comprehensive attention paid to 'ICT third-party risks' in the Digital Operational Resilience Act (DORA).[116] The question, therefore, is if NIS2, with its much broader scope than the DORA, can still offer effective supply chain cybersecurity measures.

The lack of clear supply chain-related definitions leads to several questions about the *intent* of NIS2. For instance, it explicitly excludes small and micro-sized enterprises from its scope. The Commission did not want to burden these enterprises with extensive cybersecurity investments.[117] However, virtually all companies in the EU are small enterprises.[118] Small and micro-sized enterprises are, therefore, part of nearly all supply chains, as they offer niche services or products (e.g., a camera component supplier).[119] It is therefore hardly imaginable that these enterprises would be left out of the scope of NIS2's prescribed supply chain cybersecurity measures. A clear definition of the supply chain would contribute to answering questions about the type of actors, in particular the 'direct suppliers', that IoT-using entities must adopt measures for.

---

[115] Garvey, Samuel and Kretinin (n 14); Melnyk et al. (n 34); Colicchia, Creazza and Menachof (n 42).
[116] See Ch. V DORA.
[117] Commission (n 67) 73.
[118] 'Small and Medium-Sized Enterprises: An Overview' <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200514-1> accessed 30 January 2024.
[119] Melnyk et al. (n 34) 171; Kwong and Pearlson (n 44).

Additionally, NIS2 does not indicate the *type* of security measures that 'supply chain security' requires. For instance, it states that the all-hazard risk management approach must include 'supply chain security, *including* security-related aspects concerning the relationships between each entity and its direct suppliers or service providers'.[120] It thus primarily requires 'supply chain security', which includes measures for 'security-related aspects' concerning relationships between entities and suppliers. However, the use of 'including' also leaves room for other types of measures. Therefore, chain cybersecurity under NIS2 can consist of an extensive array of cybersecurity measures (e.g., preventing hardware tampering, addressing software vulnerabilities).

Transport security illustrates the issues with such an extensive array of possible measures. International shipping companies can, to a certain extent, prevent piracy by reducing the information that is digitally available about their ships and crew, a type of online privacy management.[121] Under the abstract terms of NIS2, entities might interpret that such cargo privacy management measures are required. Such flexible interpretations have two sides: the entities might opt to take considerable security measures; however, the flexible terms of NIS2 leave room for minimally compliant measures, especially as supply chain cybersecurity is still a developing field without clear guidance from, for instance, supervisory authorities.[122]

Furthermore, NIS2 lacks a definition of the *extent* of the supply chain cybersecurity process. Supply chain cybersecurity can begin and end at different points during the production process, depending on the chosen approach. The Council of the EU, for instance, notes that supply chain cybersecurity 'begins with the sourcing of raw material and extends through the manufacturing, processing, handling and delivery of ICT products and services, including provision of support during ICT products and services' life cycle'.[123] Under this definition, IoT-using entities could require continuous security updates as part of supply chain cybersecurity, as such updates are part of the 'provision of support' during the lifecycle of the IoT device.[124] Such continuous support ensures that vulnerabilities in the IoT device's software are quickly patched, thus significantly reducing the possibility of cyberattacks. However, NIS2 does not indicate whether such support is part of its envisioned supply chain cybersecurity measures. Again, the lack of a distinct definition leaves entities with considerable interpretative leeway.

---

[120] Art. 21(2)(d) NIS.

[121] Sullivan (n 31) 241.

[122] Consider here, for instance, the overall lack of compliance with the GDPR, which stemmed from a longer line of existing data protection law and benefited, therefore, from guidance from supervisory authorities (the old Article 29 Working Party, now the European Data Protection Board). Supply chain cybersecurity does not yet enjoy such a firm status. See on the GDPR, Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 *European Journal of Risk Regulation* 502.

[123] Council of the European Union, 'Council Conclusions on ICT Supply Chain Security' (2022) 13664/22 4.

[124] European Union Agency for Cybersecurity (n 8) 17.

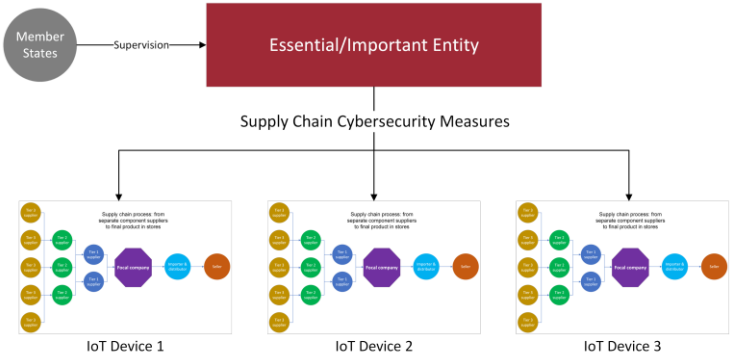
Supply chain cybersecurity in NIS2 is one element of broader cybersecurity risk management. As a result of this auxiliary role, NIS2 does not (and cannot) sufficiently define the integral components of supply chain cybersecurity. Supply chain cybersecurity remains a complex, multidisciplinary field in development; the limited regard for its intricacies in NIS2, therefore, might decrease the efficacy of the chosen measures.

5.2 The Right Responsibility in the Wrong Hands

The focal company generally governs the supply chain. The company is primarily responsible for the overall level of cybersecurity of the supply chain, for instance by requiring that new suppliers adhere to a set of security standards or best practices.[125] The focal company can properly take these measures as it stands in direct relation to first-tier suppliers. As described earlier, this collaboration is essential for proper supply chain cybersecurity.

Article 21 NIS2 does not build on these capabilities of the focal company. The provision requires IoT-using entities to take security measures, not the focal companies (i.e., IoT manufacturers) themselves. Figure 4 illustrates this hierarchy of responsibilities under Article 21.

Figure 4: NIS2 Allocation of Responsibilities



The allocation of responsibilities in Article 21 lacks regard for the diversity of supply chain actors. Focal companies are as diverse as the supply chains they manage. Frostenson and Prenkert highlight how focal companies often operate in complex networks of multiple legal entities and ownership models.[126] The IoT-using entities

[125] Melnyk et al. (n 34) 173.

[126] Magnus Frostenson and Frans Prenkert, 'Sustainable Supply Chain Management When Focal Firms Are Complex: A Network Perspective' (2015) 107 *Journal of Cleaner Production* 85.

under NIS2 are equally diverse, ranging from energy providers to the health sector. The responsibilities under Article 21, therefore, become increasingly complex. The IoT-using entities must take appropriate measures, then communicate them with the focal company or network of companies of each IoT device they use. Although NIS2 only requires the IoT-using entity to take measures in relation to its direct suppliers, these diverse direct suppliers (e.g., the focal company) must inevitably collaborate with their own suppliers for effective cybersecurity throughout the chain. This complex process does not seem practically feasible to ensure effective supply chain cybersecurity measures.

The allocation of responsibilities in NIS2 resembles the controller−processor relationship in the GDPR, as illustrated in Section 3.3. The approach in the GDPR is to keep the responsibilities with the controller as they supervise and direct the personal data processing.[127] However, privacy scholars often posit that practice does not clearly distinguish between controller and processor.[128] For instance, in cloud processing, the power of the cloud processor (e.g., Google) is often much larger than the controller that employs the cloud service (e.g., a small school).[129] The question, in that case, is whether the controller (i.e., the IoT-using entity under NIS2) should implement the data protection measures, or the cloud service as the processor (i.e., the focal company). Data protection law must protect the data subject, i.e., the individual whose data is processed. From this perspective, it is logical to ensure that the most capable entity implements the data protection measures, whether that is the controller or the processor. Google, as the processor that provides a cloud service, is presumably more capable of implementing those measures.

The law, too, should place the responsibilities of supply chain cybersecurity where they are most effective for the cybersecurity of ICT products. An alternative approach to supply chain cybersecurity, outside of NIS2, is required for this shift towards effective supply chain cybersecurity responsibilities. A stronger position for supply chain cybersecurity in product safety law, which focuses on the manufacturer instead of the user, could, in this context, offer a more effective legal framework. NIS2 thus offers a solid introduction to supply chain cybersecurity regulation, but its rules are best served as groundwork for further legislation.

6. Conclusion

NIS2 came into effect in January 2023. It introduces a set of rules aimed at the previously unregulated area of supply chain cybersecurity, which offers a response to the growing number of cyberattacks aimed at the most vulnerable partner in a co-operating network of actors. Supply chain cybersecurity is therefore closely connected to the increasing use of IoT devices, which allow data exchange between

[127] EDPB, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' 11.
[128] Peter Blume, 'An Alternative Model for Data Protection Law: Changing the Roles of Controller and Processor' (2015) 5 *International Data Privacy Law* 292; Wolters (n 85).
[129] ibid 296.

many different systems and sensors. In this article, I have sought to answer the following question: to what extent can the NIS2 supply chain cybersecurity rules help mitigate the emergence of supply chain cybersecurity problems in IoT devices used in critical sectors?

Supply chain cybersecurity is a rather novel field, with a distinct lack of definitions. A general concept of supply chain cybersecurity often requires the diverse set of actors in the supply chain, regardless of their operations, to take cybersecurity measures tailored to their organisation to protect the overall security of the supply chain.

Novel studies in the field of CSCRM offer prominent components of supply chain cybersecurity. First, organisations must focus on cyber *resilience*, i.e., the capacity of an organisation to recover after a cyberattack, as a component of cybersecurity. Second, organisations can build cyber resilience in close collaboration with partners throughout the chain, to ensure appropriate cybersecurity *investments*. Third, cybersecurity *standards* can strongly support a harmonised, collaborative approach.

NIS2 addresses ‘essential’ and ‘important’ entities, which offer critical services (e.g., hospitals, energy providers). Under NIS2, these entities must take a cybersecurity risk management approach to ensure that the network and information systems they use (e.g., IoT devices) are secure. Under this approach, they must, inter alia, focus on supply chain cybersecurity. This requirement is new in European cybersecurity law. The GDPR and the upcoming CRA, for instance, do cover respective actors in the chain and some specific cybersecurity measures, but their scope is too narrow for proper supply chain cybersecurity.

NIS2 approaches supply chain cybersecurity through an apt risk management framework. The three components of recent CSCRM studies − cyber resilience, cybersecurity investments and standardisation − form important pillars within NIS2. The supply chain cybersecurity rules in NIS2 are thus grounded on a proper risk management approach.

However, supply chain cybersecurity has only a lateral role within this risk management approach. NIS2 simply requires ‘supply chain security’ measures, which lacks awareness of the multi-faceted nature of supply chains and supply chain cybersecurity measures. In addition, it places the responsibility for supply chain cybersecurity measures on the *end user* of the IoT device (e.g., the hospital). Legislation should instead require the focal company (i.e., the IoT vendor) to maintain a secure supply chain, for instance in product-focused legislation. Future legislation should thus build on the solid groundwork of NIS2, but offer more clearly defined, concentrated supply chain cybersecurity measures aimed at the focal company.