Investment Screening Against Strategic Cyber Risks

Wouter Scherpenisse, Evert Stamhuis & Alberto Quintavalla*

Abstract

This article reviews the manner in which two types of legislation in the Netherlands, namely laws on foreign direct investment and laws on network and information security, address the risks that arise from changes in control over companies in the cybernetwork. It also identifies the potential vulnerabilities of the existing regulatory framework, which are due to the failure to adopt a sufficiently ecosystemic approach. While the EU legislation on network and information security contains appropriate and proportionate risk-management measures that ensure the security of supply chains, the Union regulation of foreign-direct-investment screening instruments appears to neglect direct suppliers and service providers.

Keywords: foreign direct investments, network and information security, cybersecurity, ecosystem, supply chain resilience.

1 Introduction

In October 2022, the international press reported on a predicament that the German federal government faced due to the growing influence of China in the Port of Hamburg.[1] The debate centred on whether the government should have intervened in the sale of 35% of the shares in the harbour facilities to the Chinese company COSCO. Geopolitical considerations were at play, in particular the question of whether the sale would cause the German economy to become more dependent on China and whether such a development would be incompatible with German national interests such as security and sovereignty.

Shortly thereafter, in June 2023, the European Commission and the High Representative published the Joint Communication on a European Economic Security Strategy.[2] Rapidly developing economic-security risks would be met by 'comprehensive' and adequate policies at the Union level and by the Member States. This approach entails coordination between the EU and its Member States when risks such as strategic dependency, as exemplified by the Port of Hamburg case, arise. According to the Communication, the following risks to economic security are most likely to require thorough assessment:

- risks to the resilience of supply chains, including energy security;
- risks to the physical and digital security of critical infrastructure;
- risks that are related to the security of technology and technology leakage;
- the risk of the weaponisation of economic dependencies and economic coercion.

Concerns about economic security have been studied extensively. Bulten and her co-authors concluded that foreign purchases of shares in companies that are embedded in the vital infrastructure of a country can affect national security in a way that merits state intervention.[3] They argued that company law does not contain sufficient safeguards against those risks and that sector-specific laws should permit the *ex ante* screening of investments. Sector-specific laws of this kind could, however, clash with other principles and norms. For instance, from an EU perspective, the control that Member States would exert over foreign investment could be considered to interfere with the free flow of capital on the common market. For this reason, the EU institutions had to strike a balance between potentially conflicting interests. This balancing act resulted in the adoption of the Foreign Direct Investment Regulation (the FDI Regulation), which harmonises laws on critical investments and serves as the topic of this special issue.[4] Under the body of law that has accumulated under the Regulation, the freedoms of private corporations can be limited for reasons of national security that are defined in national screening instruments.

* Wouter Scherpenisse, LL.M is a PhD candidate at the School of Law of the Erasmus University Rotterdam, the Netherlands. Evert Stamhuis is Professor at the School of Law of the Erasmus University Rotterdam, the Netherlands. Alberto Quintavalla is Assistant Professor at the School of Law of the Erasmus University Rotterdam, the Netherlands. Corresponding author: scherpenisse@law.eur.nl.

1 www.reuters.com/markets/deals/german-cabinet-approves-investment-by-chinas-cosco-hamburg-port-terminal-sources-2022-10-26/ (last visited 21 June 2023).

2 https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3358 (last visited 21 June 2023).

3 C.D.J. Bulten, e.a., *Vitale vennootschappen in veilige handen. Een wetenschappelijk onderzoek in opdracht van het WODC naar de wijze waarop (buitenlands) aandeelhouderschap gevolgen kan hebben voor de nationale veiligheid* (2017).

4 European Parliament and Council Regulation 452/19, OJ 2019 L 79I/1 (FDI Regulation).

doi: 10.5553/ELR.000252

The EU FDI instruments and the related national legislation are intended to prevent undesirable foreign control over key companies. Screening focuses on risk management at companies whose operations ought to be protected even in times of geopolitical tension. However, close scrutiny of the vital sectors of the European economy reveals that the risk of undesirable interference is not limited to changes in control. The role of interconnected counterparties entails numerous other perils.

Companies with digital outputs provide some of the most salient examples.[5] Digital service companies of all kinds operate in hyperconnected supply chains.[6] It matters little whether the company is active in a predominantly digital market, such as the stock exchange, or in an analogue sector such as air traffic or harbour facilities. Digital service companies are hubs in these networks; consequently, their activities are also networked. For instance, Portbase, which provides digital-communication services at the Port of Rotterdam,[7] is not only a service-provision hub but also relies on numerous suppliers. It is safe to assume that more than a few of those suppliers play an essential role in the daily operations of the Port.[8] At companies such as Portbase, the risk of undesirable foreign interference is not limited to the prospect of a foreign party assuming control. A change in control over one or more of its key suppliers would also leave the firm vulnerable because switching suppliers is often highly difficult.

For these reasons, we studied the investment-screening legislation. The questions that we seek to answer have to do with the extent to which screening can detect risks that are not related directly to control over the target company. If it cannot, the legislation may generate a partially false sense of security. The analysis that we present focuses on FDI legislation and the additional screening laws that apply to key companies.[9] Given that these additional laws tend to apply in Member State jurisdictions, we chose to focus on the Netherlands.

Another domain of EU risk regulation covers cyberservices that are key for financial markets, harbours and airports. Central to that domain is the Network and Information Security Directive (the NIS Directive), which is now being updated.[10] Important participants in the network and the information ecosystems of key sectors are subject to its provisions.[11] They have duties of care that require them to respond proactively when potential changes in control over companies or suppliers are liable to affect their performance.[12] These provisions will be extended by the updated NIS2 Directive. The question is how and to what extent the risks of undesirable control over key economic entities, which may be neglected under the extant investment-screening mechanisms, may be covered by network and information security legislation.[13] The second question that this article addresses, therefore, is how the providers of key cyberservices respond to the prospect of loss of control. What are the normative expectations about the relevant actors, the boards of key companies and the authorities that are tasked with preventing foreign interference and with protecting national sovereignty? The analysis uncovers the ways in which companies must respond to threats, that is, it explains what policies and actions are compliant with the relevant regulations. We also inquire whether the investment-screening authorities have access to appropriate instruments, and, after examining the two mechanisms separately, we identify lacunae in risk regulation and potential means of plugging them.

The questions are amenable to the application of a doctrinal legal methodology. We analyse textual sources; legislative documentation, including publicly available national-level policy reports; and, where possible, scholarly publications on the topics of interest. Given the recency of the topic and its legislative background, this article represents an initial attempt at exploration.

Our contribution is structured as follows: Section 2 examines the FDI mechanism at the EU level and the additional legislation that has been passed at the national level. Section 3 focuses on the NIS Directive and the legislation that implements it in the Netherlands. We illustrate the economic-security issues that emerge in practice by referring occasionally to the example of Portbase. Section 4 summarises the main findings and identifies avenues for further research.

2 Investment Screening in the EU and at the National Level

2.1 The FDI Regulation

The EU has always had the difficult task of balancing the efficiency gains from having a market that is open to foreign investment against the need to protect internal

5 Cyberspace can be conceptualised as 'a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies' (D.T. Kuehl, 'From Cyberspace to Cyberpower', in F.D. Kramer, S.H. Starr & L.K. Wentz (eds.), *Cyberpower and National Security* (2009) 24, at 28.

6 See e.g. W. Bauer, M. Hämmerle, S. Schlund & C. Vocke, 'Transforming to a Hyper-connected Society and Economy – Towards an "Industry 4.0"', 3 *Procedia Manufacturing* 417 (2015); I. Tasheva and I. Kunkel, 'In a Hyperconnected World, Is the EU Cybersecurity Framework Connected?', 21 *European View* 186 (2022); S. Schauer, N. Polemi, & H. Mouratidis, 'Mitigate: A Dynamic Supply chain Cyber Risk Assessment Methodology', 12 *Journal of Transportation Security* 1 (2019).

7 www.portbase.com/en/about-us/ (last visited 21 June 2023).

8 www.portbase.com/softwareleveranciers/ (last visited 21 June 2023) provides a table in which more than 50 software providers are listed. We could not access more substantial information about the nature of the contracts, which could have been for the one-off delivery of software or for software as a service. The latter entails permanent connection at the system level.

9 On the definition of 'vital companies', see Art. 1 Wet Vifo (*Stb.* 2022, 215).

10 European Parliament and Council Directive 2555/22, OJ 2022 L 333/80 (NIS2 Directive).

11 On scope, see Art. 2 NIS2 Directive.

12 As discussed in Section 3.2.

13 See *Kamerstukken II* 2020/21, 35880, nr. 3, at. 13 and 15 (Explanatory Memorandum to the Act that is discussed in Section 2.2).

strategic and security interests. On the one hand, ensuring free movement of capital would, or so the argument runs, ensure that capital is allocated optimally, resulting in economic growth.[14] On the other hand, numerous public interests are worthy of protection, regardless of the potentially negative impact that protecting them may have on free trade.

Against this background, the EU adopted its Regulation on the screening of foreign direct investments in March 2019. That Regulation is liable to obstruct some foreign investments.[15] It entered into force on 11 October 2020 (as per Art. 17), and it responds to the concerns that the European Commission highlighted in the Explanatory Memorandum that accompanies it.[16] Specifically, the Commission acknowledged that the regulation 'provides a policy response to protect legitimate interests with regard to foreign direct investments that raise concerns for security or public order of the Union or its Member States'. These concerns pertain to the security of critical infrastructures such as the Port of Rotterdam.[17]

Surprisingly, neither the memorandum nor the regulation are clear on the nature of the specific interests or the type of foreign companies that may 'raise concerns for security or public order' in the EU. Instead, the FDI Regulation limits itself to a reference to 'companies that develop technologies or maintain infrastructures that are essential to perform critical functions in society and the economy'.[18] Cyberinfrastructure companies are obviously among the most germane examples of this class of businesses.[19]

The FDI Regulation also emphasises the importance of screening mechanisms for security and public order. They 'provide legal certainty for Member States' and must 'ensure Union-wide coordination and cooperation in the screening of foreign direct investments' that are likely to affect security or public order.[20] One may wonder whether the public interests in question are sufficiently protected by the FDI Regulation. Does the implementation of the Regulation suffice to mitigate the potential risks to security or public order that stem from foreign direct investment? Does the EU instrument cover all of the instances in which a foreign investor can create risks for critical infrastructure in the Member States? In our view, these questions should be answered in the negative. For instance, not all types of transaction are covered by the FDI regulation. The term 'foreign direct investment' is defined as

> an investment of any kind by a foreign investor aiming to establish or to maintain lasting and direct links between the foreign investor and the entrepreneur to whom or the undertaking to which the capital is made available in order to carry on an economic activity in a Member State, including investments which enable effective participation in the management or control of a company carrying out an economic activity (Art. 2(1)).

The implication is that the FDI Regulation primarily addresses instances in which investors obtain the ability to actually manage or control a company that is labelled 'vital'. In other words, intra-EU direct investments and investments that do not enable 'effective participation' in a company (such as portfolio investments) are not subject to the Regulation.[21] This limited applicability means that some (foreign) investments that would pose a threat to internal strategic and security interests are left unregulated. For instance, it would be possible, in principle, for several (foreign) investors that do not comply with the provisions of the Regulation to participate effectively in a company jointly, provided that none of them does so individually.

There are also other examples of the inharmonious approach to investment screening in the EU. An investor from a third country can invest through a company that is domiciled in a Member State. Although the FDI Regulation captures such situations partially in virtue of its anti-circumvention clause, Article 3(6) falls short of guaranteeing a common EU approach. The Article provides that it is the Member States that should adopt measures to 'identify and prevent circumvention of the screening mechanism and screening decisions'. Accordingly, the scope of application of the FDI Regulation is in the remit of the Member States to a significant degree, and its operation depends on national regulatory choices.

Another consideration that is critical to the present ends is that the FDI Regulation appears to be designed chiefly to protect companies that are labelled 'vital'. Regulatory attention is directed mainly at the likely impact of foreign direct investment on individual legal entities. This said, the role of supply chains in critical infrastructure is not altogether neglected. Reference is also made to the possible effects of foreign direct investment on the 'supply of critical inputs, including energy or raw materials, as well as food security' (Art. 4(1)(c)). Nevertheless, the ecosystemic view is underdeveloped in the regulation. This poses several problems for the regulation of risk to 'critical inputs' at both the EU and the Member State level. The implementation of the FDI Regulation is highly dependent on the will of the Member States; however, critical suppliers can be dis-

14 S. Hindelang, *The Free Movement of Capital and Foreign Direct Investment: The Scope of Protection in EU Law* (2009), at 19.
15 Regulation 2019/452 (FDI Regulation).
16 Commission Proposal 0024/17 (FDI).
17 *Ibid*., at 2.
18 *Ibid*., at 10.
19 See Art. 4(1) FDI Regulation.
20 Recital 7 to the FDI Regulation.
21 See, in this regard, Recital 9 to the FDI Regulation as well as the Communication from the Commission on Guidance to the Member States concerning foreign direct investment and free movement of capital from third countries, and the protection of Europe's strategic assets, ahead of the application of Regulation (EU) 2019/452 (the FDI Screening Regulation). The latter document acknowledges that portfolio investments can become relevant to the security or public order of a Member State when 'they represent an acquisition of at least qualified shareholding that confers certain rights to the shareholder or connected shareholders under the national company law (e.g. 5%)'.

doi: 10.5553/ELR.000252

persed across the Union. It is the Member States that are called to devise effective regulations that address the risks that foreign direct investments can create. The screening criteria provide a striking example of this tendency. Article 4 of the FDI Regulation contains an open-ended list of factors that the Member States (and the Commission) should take into account before reaching decisions on screening. Those decisions are, in fact, a Member State competence and a matter for national screening legislation (see also Art. 3(1) and Recital 12). In order to prevent harm from inertia and to generate an additional layer of protection for the EU internal market, Article 8(1) enables the Commission to issue non-binding opinions whenever a foreign direct investment can affect projects or programmes of Union interest.[22]

That the FDI Regulation mostly demands action from Member States is also evident from Article 6, which requires Member States to communicate 'any foreign direct investment in their territory that is undergoing screening' and to share all relevant information, as set out in Article 9(2), with the other Member States and the Commission.[23] At the same time, the Member States and the Commission can request additional information (Art. 6(6)) as well as comment on foreign direct investments on the territories of other Member State that have not been screened but may affect their internal security or public order (Art. 7). Once again, these provisions leave significant leeway to the Member States.[24]

In short, the EU legislation shifts most of the responsibilities for overseeing changes in control over target companies to the Member States. Put bluntly, the FDI Regulation contains open-ended provisions that Member States are expected to operationalise. In the next subsection, we zoom in on the Netherlands in order to develop an example of the implementation of the FDI Regulation in a specific Member State.

2.2 National Complements

Turning to actual oversight mechanisms, the Netherlands promulgated a minimal-implementation Act on 18 November 2020. It was published in *Stb*. 2020, 491, and entered into force on 4 December 2020. The Act does not deviate from the criteria from the Regulation and simply contains a mandate for the national authorities to enforce its provisions. The authorities in question are various central-government ministers, who can task the Office for Investment Screening (*Bureau Toetsing Investeringen*) with coordinating and executing relevant tasks. As far as enforcement is concerned, the Act provides for purely administrative-law sanctions through Article 6. Injunctions that are backed with penalties for default are the favoured remedy. For example, such injunctions may be granted when the information requirements under Article 9(4) of the FDI Regulation are not fulfilled.

Beyond the legislation that implements the FDI regulation,[25] the Netherlands also introduced a national supervision instrument for the protection of national security and sovereignty in relation to vital providers or providers of sensitive technology. That instrument is meant to implement the FDI mechanism and, to a certain degree, to complement it. The corresponding Act of Parliament was promulgated on 18 May 2022, published in *Stb*. 2022, 215, and entered into force on 1 June 2023.[26] This Act on the Security Screening of Investments, Mergers and Take-overs is intended to provide generic procedures and criteria that add to the limited array of sectoral instruments that were previously available to the authorities (Art. 5(1)). Those instruments applied to the telecommunications network and to water supply.[27] The Act imposes duties on both the investing party and the target enterprise, which include the duty to report an intended acquisition of control over a vital provider (Arts. 2 and 11). Such reports trigger assessments by the Office for Investment Screening. The purpose of the assessments is to determine whether the facts of the case fall under the scope of the Act and, if so, whether the Minister of Economic Affairs and Climate Policy should intervene (Arts. 10 and 12 *et seq*.). The interventions that are available to the Minister include banning an acquisition. The Act also contains an enforcement mechanism and a remedial procedure that extends legal protection to individual actors.

It may be necessary to explain the conditions under which a company may become subject to this mechanism. The status of 'vital provider'[28] is defined by Article 7 and the bylaw from Article 7, para 11. The Act is meant to result in *ex ante* risk assessments for companies that provide vital services.[29] Only the companies that are defined in the legislation to which Article 7 refers fall under the scope of the Act. For an acquisition to be caught by the Act, a proposed change in control, broadly defined, should compromise its productivity or result in strategic dependence. Consequently, even though the risk that arises from the acquisition of control over an upstream company in the supply chain may fall under the definition of a 'threat to national security/

22 See also Recital 19, which state explicitly that final decisions remain 'the sole responsibility of the Member State'.

23 Note that Member States, in cooperation with the concerned company, are responsible for acquiring information when they monitor foreign investments.

24 Recital 4 to the FDI Regulation.

25 *Uitvoeringswet Screeningsverordening buitenlandse directe investeringen, Wet van 18 november 2020* (*Stb*. 2020, 491).

26 *Besluit van 4 mei 2023 tot vaststelling van het tijdstip van inwerkingtreding van de Wet veiligheidstoets investeringen, fusies en overnames, het Besluit veiligheidstoets investeringen, fusies en overnames en het Besluit toepassingsbereik sensitieve technologie* (*Stb*. 2023, 174).

27 As far as telecommunication is concerned, the Act (*Wet ongewenste zeggenschap telecommunicatie* (*Stb*. 2020, 237)) provides for supervision over changes of control over companies. For water supply, the relevant Act (*Drinkwaterwet* (*Stb*. 2009, 370)) contains a ban on privatisation. See the commentary in *Kamerstukken II* 2020/21, 35880, nr. 3, at 14, 19 and 135.

28 Since we focus on companies that operate in the civil cyberinfrastructure, we do not examine the provisions on sensitive military technologies that are caught by the Act directly or indirectly (in virtue of their dual use) (Arts. 4 and 8).

29 *Kamerstukken II* 2020/21, 35880, nr. 3, at 12.

sovereignty',[30] the Act does not apply to that company unless it is a vital provider.

Furthermore, the Act only applies to the acquisition of control by way of investment, merger, joint venture, severance or legal actions that have the same effect, as listed in Article 2. Any other form of leverage or interference that threatens the continuous performance of the vital provider is apparently not covered. When a foreign investor obtains control over a supplier of crucial services (within or outside of national borders) such as Portbase, there is no legal justification for triggering the mechanism of the Act. Our assumption is that the 'vital provider' label does not automatically apply to the counterparties of established vital providers. Accordingly, we infer that few of the vulnerabilities of cyberservice companies can be addressed by the investment-screening mechanism.

In sum, the managers of a target enterprise that is a vital provider need to observe reporting duties when control over the company is in the process of changing hands. Those duties pertain both to the actions that require managerial involvement and cooperation and to gradual transfers of control that can be outside of the purview of managers, such as trades in the shares of listed companies. Effectively, the board must know its investors not just when discrete sales of shares occur but also when its equity is traded on the stock exchange. The mechanism relies heavily on the information that the investor and the target company provide.[31] The investment-screening mechanisms, taken in their totality, do not, however, require the boards of vital providers to monitor the parties that control or influence their essential suppliers. As stated explicitly in the Explanatory Memorandum, other instruments are in place that can preserve the national interests of security and sovereignty in cases in which companies operate in networks and within information infrastructures. We discuss those instruments in Section 3.

3 Network and Information Security

3.1 First Regulatory Initiative

The EU legislature produced several instruments that purport to improve digital and thus general resilience within the context of the Cybersecurity Strategy of the European Union.[32] One of these instruments is the Network and Information Security Directive 2016/1148 (the NIS Directive).[33] The NIS Directive is premised on the notion that

> a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers

is required in order to respond effectively to digital challenges,[34] thereby 'contributing to the Union's security and to the effective functioning of its economy and society'.[35] In that sense, the objectives of the Directive and the FDI Regulation show similarities.[36]

This approach resulted in the formulation of several main aims, which are mentioned in Article 1(2) of the NIS Directive. For example, the Member States would adopt national strategies for the security of network and information systems. Security and notification requirements for operators of essential services (OESs) and digital service providers would be set, and national competent authorities, single points of contact and Computer Security Incident Response Teams would be formed and given tasks that would be related to the security of network and information systems.

Article 5 NIS and Annex II (2c) provide the Member States with guidelines on the identification of OESs.[37] As far as the context of our study is concerned, this mandate was fulfilled by the *Wet beveiliging netwerk- en informatiesystemen* (*Wbni*; the English translation is 'Act on Network and Information System Security').[38] Article 5(1) *Wbni* delegates responsibility for identification tasks to a governmental Order in Council. Those tasks are fulfilled by the *Besluit beveiliging netwerk- en informatiesystemen* (*Bbni*).[39] Portbase doubtless falls outside of the OES category because the law does not designate it as an OES – another actor in the Port is mentioned instead. The implementation of the NIS2 Directive is likely to have a considerable impact on this classification. The shift from OESs to 'essential and important entities' and the omission of the term 'operator' that it entails result in a wider range of actors being caught by the provisions. The foregoing should not be taken to imply that the importance of cyber risks was ever neglected in relation to the Port.

The recently published Dutch strategic-policy document *Nederlandse Cybersecuritystrategie 2022-2028* (NLCS) reveals much about the national strategy.[40] The NLCS explicitly mentions the significant dependency of

30 The Explanatory Memorandum states that Art. 4(1)(c) of the FDI Regulation was included in the Act because of the broader definition of national security (Commission Proposal 0024/17 (FDI)); *Kamerstukken II* 2020/21, 35880, nr. 3, at 74.

31 *Kamerstukken II* 2020/21, 35880, nr. 3, at 33.

32 Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN [2013] 1 final (52013JC0001).

33 European Parliament and Council Directive 1148/16, OJ 2016 L 194/1 (NIS Directive).

34 Directive 2016/1148 (NIS Directive), Recital 6.

35 Directive 2022/2555 (NIS2 Directive), Recital 1.

36 Regulation (EU) 2019/452 (FDI Regulation), Recitals 1 & 3.

37 It is unnecessary to discuss the 'digital service providers' category.

38 *Wet beveiliging netwerk- en informatiesystemen van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU)* 2016/1148 (*Stb.* 2018, 387).

39 *Besluit van 17 maart 2021 tot wijziging van het Besluit beveiliging netwerk- en informatiesystemen (aanwijzing vitale aanbieders en nadere regels over beveiliging aanbieders van een essentiële dienst)* (*Stb.* 2021, 160).

40 Ministerie van Justitie en Veiligheid, *De Nederlandse Cybersecuritystrategie 2022-2028. Ambities en acties voor een digitaal veilige samenleving* (2022).

doi: 10.5553/ELR.000252

the Netherlands on the Port of Rotterdam. The text implies that Dutch digital resilience remains insufficient.[41] In addition, the NLCS mentions that, in order to establish an 'open, stable and secure digital world', the digital ecosystems on which the country depends must be seen as parts of a globally interconnected network.[42] This proposition has several implications. Dependence on vital entities such as the Port of Rotterdam is obviously not a phenomenon that is restricted to the borders of individual Member States. Since geopolitical goals are increasingly being pursued through offensive cyberoperations and since Chinese operations of this kind are unparalleled in magnitude, the Port of Rotterdam should be particularly careful when Chinese state-owned shareholders enter its cybersecurity network.[43] Furthermore, the security assessments of entities within the Port of Rotterdam should not be limited to the harbour or to the providers of particular services.

The NIS legislation subjects actors who fall within the scope of the OES concept to several obligations. Article 14 NIS lists the main security and incident-notification requirements. The measures fall into two categories. First, risk-management measures must be appropriate and proportionate, which shifts much of the responsibility to the providers of essential services that are mentioned in Recital 44 to the NIS Directive.[44] This approach has been transposed directly onto Article 7(1) *Wbni*. Second, Article 7(2) *Wbni* contains guidelines as well as 'measures preventing and minimising the impact of incidents', which must be appropriate. Article 8 *Wbni* reiterates this proposition and therefore also places much responsibility on operators. However, neither risk-management nor incident-prevention measures are left to the exclusive competence of those operators. A governmental Order in Council may define more specific rules.[45] Even within this framework, little attention is paid to the vulnerabilities of supply chains.[46] This limitation, which evidently extends to national implementation measures, reflects the spirit of the FDI instruments.

The limited scope of the *Wbni* has not gone unnoticed. The enforcement authorities in the Netherlands have found that the focus on OESs as isolated entities does not cohere with the risks that emerge in actuality. In 2022, the competent Inspectorate noted that focusing exclusively on OESs would be insufficient in the future. Even extending monitoring to direct suppliers would not be adequate. Instead, an ecosystemic approach was thought to be necessary.[47] Due to the interdependencies between digital ecosystems that are caused by, among other things, the outsourcing of IT processes,[48] supervisory authorities ought to account for more links in supply chains in order to achieve actual supply chain resilience.[49] Such an approach is more likely to account for the proposition that 'each new object connected to the Internet will represent an additional entry point to the digital ecosystem that will have to be secured'.[50] If sufficient cybersecurity is to be attained, the practice of paying attention to the most eye-catching entities selectively must be replaced by a weakest-link approach. Currently, focusing on individual OESs under the NIS Directive creates too many cracks in the Dutch cybershield.

The emergence of this more comprehensive approach should be examined against the backdrop of the *NotPetya* attack and the *SolarWinds* hack. *NotPetya* was a large-scale uncontrolled offensive attack on Ukraine in 2017. It had a global impact.[51] In the *SolarWinds* hack of 2020, which was a more controlled cyberespionage operation, hackers found backdoors that enabled them to penetrate supply chain operations.[52] Both cyberattacks exemplify the vulnerabilities of popular digital systems that can be exploited when insufficient attention is paid to supply chain resilience. *SolarWinds* had to do with controlled access through software suppliers, and *NotPetya* had to do with system updates. ENISA illustrated these supply chain vulnerabilities in a recent publication and provided further examples of similar attacks.[53] These examples show that supply chain issues call for harmonised responses because they transcend national security issues. Why would attackers focus on highly protected entities that are bound to strict legal frameworks when backdoors in other Member States may be far easier to exploit? The NIS may have been implemented a few years before the crystallisation of a political will to create a level playing field in EU cyberspace.[54] Its successor, however, will advance harmonisation further.

41 *Ibid*., at 10, 12.
42 *Ibid*., at 7.
43 NCTV, *Cybersecuritybeeld Nederland 2022* (2022), at 22-23.
44 See Directive 2016/1148 (NIS Directive), Recital 46.
45 Art. 9 *Wbni*.
46 The Dutch legislator partially anticipated this shortcoming and revisited the *Wbni* in a way that makes sharing information with non-vital entities possible under certain circumstances (*Kamerstukken II* 2021/22, 36084, nr. 3, at 2).
47 Ministerie van Economische Zaken en Klimaat, *Samenhangend inspectiebeeld cybersecurity vitale processen. 2021-2022* (2022), at 15.
48 Z. Bederna and Z. Rajnai, 'Analysis of the Cybersecurity Ecosystem in the European Union', 3 *International Cybersecurity Law Review* 35, at 43 (2022); S. Prawesh, K. Chari & M. Agrawal, 'Industry Norms as Predictors of IT Outsourcing Behaviors', 56 *International Journal of Information Management* (2021).
49 On the concept of supply chain resilience, see the works of Ponomarov and Holcomb (S.Y. Ponomarov and M.C. Holcomb, 'Understanding the Concept of Supply Chain Resilience', 20 *The International Journal of Logistics Management* 124 (2009)).
50 B. Dupont, 'Cybersecurity Futures: How Can We Regulate Emergent Risks?', 3 *Technology Innovation Management Review* 6, at 9 (2013).
51 A. Greenberg, *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (2019), at 179-183; The global effect of *NotPetya* also affected the Port of Rotterdam, where several container terminals were shut down www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/ (last visited 21 June 2023).
52 M. Willett, 'Lessons of the SolarWinds Hack', 63 *Survival* 7 (2021).
53 ENISA, *Good Practices for Supply Chain Cybersecurity* (2023), at 36-37.
54 Smeets discussed the issue of the level playing field in cyberspace in (M. Smeets, *No Shortcuts. Why States Struggle to Develop a Military Cyber-Force* (2022), at 33-49.

3.2 The NIS2 Update

The NIS2 Directive accounts for this broader border-transcending ecosystemic approach. When the Directive is implemented, several changes will occur, with varying impacts. One of these changes concerns the scope of the Directive. Instead of applying to OESs and digital service providers, the NIS2 Directive differentiates between essential and important entities (Art. 3). Since the Directive has harmonisation-related goals, the categorisation of these entities is overviewed in the first two annexes to its text. Centralisation is favoured over subsidiarity, unlike in the NIS Directive. This more centralised approach to network and security legislation is in apparent contrast to that which was adopted in the FDI legislation, which proceeds from the assumption that most of the implementing legislation should be developed by the Member States. The justification of this difference in approach is not obvious, especially given the similarity of the general aims of the two frameworks, which purport to create a secure EU (market).

An examination of the scope of the NIS2 Directive and the entities in Annex 1 reveals that Portbase would be caught by its provisions. The Port of Rotterdam contains many more essential entities than it contains OESs. Annex I provides for three relevant categories of essential entities, namely inland, sea and coastal passenger and freight water-transport companies; managing bodies of ports and operators of vessel-traffic services.[55] As a consequence, instead of a single identified entity, there will be around 150 companies that are treated as essential.[56] Given the enhanced obligations, responsibilities[57] and supervision and enforcement measures,[58] it is clear that the implementation of the NIS2 Directive will bring a new set of companies into the scope of the mechanism, including the providers of key digital services to the Port.

This broader ecosystemic approach affects not only the number of entities that should abide by the provisions of the NIS2 Directive but also the content of their obligations. The cybersecurity risk-management measures from Article 21 NIS2 supply a relevant example. Article 21(2d) NIS2 states that the all-hazard approach to protecting network and information systems and their physical environment includes 'supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers'. Paragraph 3 of that Article adds that

> Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.

As noted previously, a narrow focus on entities and their 'direct suppliers' might be insufficient. The NIS2 Directive stipulates that 'entities should also address risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem'.[59] This ecosystemic approach accords more attention to the weakest links in cybersecurity and therefore provides a higher degree of protection from digital threats. The Dutch implementation Bill has not been publicised yet, so some caution is warranted. Thus far, it can only be assumed that Portbase will fall within the scope of the NIS2 system. The probability that a single malicious supplier of software can bring down a global digital services system as if it were a house of cards will no longer be underestimated, and the efforts that are directed at the prevention of such occurrences will no longer vary arbitrarily from case to case. Foreign and domestic software suppliers will be monitored adequately, and digital backdoors will be governed as significant cyber risks. The NIS2 Directive stipulates that the security of the supply chain and the broader ecosystem must be considered.[60] Even more specifically, an ENISA publication contains the following stipulation: 'Entities shall identify and assess supplier risk as an integral component of their risk management approach' mentioning and among other things 'country-specific information (e.g. threat assessment from national security services etc).'[61] Thus, the new starting point will be that the suppliers of unfriendly foreign entities are, in principle, to be denied access to the backdoors of essential and important organisations throughout the Union. For Portbase, this may mean that, for example, software suppliers from countries that have adopted offensive strategies according to the Dutch General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdient*), such as China and Russia, would not be allowed to enter the market.[62]

In the context of supply chain resilience, cybersecurity risk-management measures need to be considered and can be incorporated into contractual arrangements.[63] As Recital 85 to the NIS2 Directive notes,

> Essential and important entities should, in particular, be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.

This ecosystemic approach extends beyond technological dependencies in the supply chain and thus brings

55 This only concerns the transport sector.
56 www.ferm-rotterdam.nl/nl/verslag-nis2 (last visited 21 June 2023).
57 Art. 20 NIS2 Directive, cf obligations such as risk management and impact prevention (Art. 21) and reporting obligations (Art. 23).
58 See Directive 2022/2555 (NIS2 Directive), Chapter 7.
59 Directive 2022/2555 (NIS2 Directive), Recital 88.
60 Directive 2022/2555 (NIS2 Directive), Recitals 85, 88 & 90.
61 ENISA, *Good Practices for Supply Chain Cybersecurity* (2023), at 22.
62 Algemene Inlichtingen- en Veiligheidsdienst, *AIVD Jaarverslag 2022* (April 2023), at 29.
63 Directive 2022/2555 (NIS2 Directive), Recital 85.

doi: 10.5553/ELR.000252

the risks that are outlined in this article, such as strategic dependency in ecosystems, into view. Recital 90 refers to a high-level risk assessment that accounts for strategic dependencies of this kind and calls specific actors to formulate a risk-mitigation strategy on its basis:

> Potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, in particular in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, in particular in the case of technological lock-in or provider dependency.

In the NIS2 system, the board of a company that is an essential and/or an important entity, such as Portbase, must be familiar with those who invest in the suppliers of the company and the risks that are connected to the suppliers which are embedded in the service-delivery ecosystem. As soon as the targeting of such suppliers generates strategic threats for the vital company that affect its control over its own service provision or its continuous functioning, the board needs to take action by terminating the contractual relationship and finding an alternative supplier. If interpreted as a proactive duty of care, this requirement entails the inclusion of clauses in supplier contracts that permit immediate termination upon the discovery of strategic threats of the kind described above. There should also be policies for preventing vendor lock-in and for enabling switching to alternative lower-risk suppliers. Otherwise, the unavailability of a backup plan would, to a certain extent, limit compliance with the duty to terminate immediately because such terminations would endanger the secure and continuous delivery of the service.

4 Discussion, Conclusion and Further Research

Society is currently learning to cope with the reality of digitalisation and its impact on the economy. An important feature of digitalisation is the existence of networks that create an ecosystem of nodes, hubs and connections in which risks are magnified. This interconnection means that companies should be seen not as isolated entities but as parts of a network that may require more integrated regulatory responses.

In this article, we sought to analyse the risks that emerge in consequence of strategic dependencies after changes in control over companies in cybernetworks. Specifically, we analysed the applicability and suitability of two types of legislation. One governs the screening of foreign direct investment, and the other creates duties of care for entities in vital-sector cybernetworks. In our analysis of the investment-screening instruments, we concluded that those laws mainly target single companies and leave considerable leeway to the Member States of the EU. In this first assessment, we notice that little attention is paid to supply chains and network effects. The threats that result from a proposal to take over a key supplier can only trigger the operation of the screening mechanism and raise the prospect of intervention if the target company itself falls within the scope of the legislation at either the EU or the Member State level. For highly connected cyberservices companies, this potential lacuna undermines safeguards against strategic dependencies.

The updated network and information security legislation that has now been adopted at the Union level and is awaiting implementation in the Member States is an important step towards a cyber-resilient EU economy. Ecosystemic approaches strengthen the EU cybershield and reduce opportunities for the exploitation of backdoors, which can be catastrophic. Not only does the NIS2 Directive include more entities in its scope, but it also amplifies and strengthens the minimum-security measures that should be adopted. In this context, supply chain resilience and a sensitive approach to the wider ecosystems of which the regulated entities form part are important desiderata.

Under the investment-screening system that emerges from the legislation, the board of a vital-service provider needs, first of all, to be familiar with its investors. As soon as a change in control is in contemplation, the company must comply with its duties under the FDI Regulation and Member State legislation such as the Act (*Stb*. 2020, 491) that we discussed. Under the NIS2 system, the board also needs to be acquainted with those who invest in its suppliers and with the risks that are related to the suppliers which are embedded in the service-delivery ecosystem. If there is a strategic threat to the control that the vital company exercises over its own service provision or to its continuous functioning, the board needs to act. However, the investment-screening mechanism of the FDI Regulation is only activated when the supplier is also a vital company. If it is not, then it is better to terminate the contractual relationship and to find a replacement. The shift from this *ex post* obligation to a proactive duty of care in the NIS2 Directive means that contracts with such suppliers must provide for immediate termination upon the discovery of threats. In addition, policies that prevent vendor lock-in must be put into place. A rapid switch to a new supplier and scaling up the provision of the service in a diversified-supply context need to be realistic prospects. Otherwise, the failure to formulate a backup plan would render reliance on termination clauses impracticable. This article did not examine the techno-empirical situation, which might reveal evidence of inter-relations that make the prospect of termination remote. In that case, even more precautions should be taken.

The analysis of the two types of legislation revealed the potential vulnerabilities of the current FDI regime. The all-hazard approach to determining appropriate and proportionate risk-management measures in the NIS2 Directive includes supply chain security. Even relationships between entities and their direct suppliers or service providers should be taken into account. Conse-

doi: 10.5553/ELR.000252

quently, the status of (foreign) suppliers of software or coded components is part of the assessment of prospective risk-management measures. In the contemporary geopolitical context, state-owned companies in China and Russia should therefore be excluded from the supply chain for essential services. Considering that this all-hazard approach is among the overarching aims of the legislation, it remains unclear why the Dutch investment-screening mechanism does not include a similar provision. This said, the salience of this legally framed argument is open to question – the mechanisms complement each other in practice. This proposition will continue to hold if the contractual arrangements in supply chains and networks are drafted so as to accord with the NIS2 duties, which would make the affected entities unattractive as takeover candidates; consequently, the investment-screening mechanism would not be needed in practice.

We did not account for the interaction between the legislation that we reviewed and the instruments of risk regulation that govern software markets, such as the future AI Act of the EU. The risks to which Article 9 of the draft AI Act refers indicate that the importance of strategic economic security, which may fall outside of their scope, has been neglected.[64] In that case, legal complexity will increase for companies that operate in the cyber-infrastructure and employ AI.

Research that compares suppliers inside and outside of the EU is needed. Comparisons between the Union and the national level would also generate further knowledge about the adequacy of risk responses. The national implementation of the NIS2 Directive, which should be completed by 2024, will also require further study. Although the level of harmonisation under that legislation is much higher than under the previous Directive, it will be interesting to see what specific duties of care the Member States will distil from the ecosystemic approach. One question that studies on that topic would have to answer is whether the enhanced scope of the regime means that supervisory authorities must rearrange their supervision and enforcement mechanisms. If the answer is in the affirmative, the national interpretations of the relevant norms may come to diverge.

The ecosystemic perspective that animates the NIS2 Directive would be somewhat arbitrary if it was limited to matters of scope. The importance of harmonisation for the protection of EU interests transcends the ends of the NIS2 regime. All threats to vital infrastructure, including digital ones, should be a matter of concern across the Union. Therefore, the lack of a harmonised and ecosystemic approach to mechanisms such as the FDI Regulation casts the completeness of that instrument into doubt. This incompleteness may undermine effectiveness at the company level. Accordingly, a way should be found to complement the FDI Regulation with the NIS2 Directive. It is possible that, in the very near future, a more comprehensive FDI Regulation that creates a level playing field will emerge. That debate is obviously for a different day. For now, it should suffice to say that integrating the FDI Regulation and the NIS2 Directive would conduce to the safeguarding of the ecosystemic approach. Our recommendation for the European Commission is to take this consideration into account when it reviews the FDI screening instruments.

64 For further details, see J. Schuett, *Risk Management in the Artificial Intelligence Act* (2022), https://arxiv.org/abs/2212.03109 (last visited 21 June 2023).

doi: 10.5553/ELR.000252