Port politics: Strategic autonomy and European ports

A case study on Chinese involvement

Xiaoxue Martin
Bart Kuipers
Frans-Paul van der Putten

CKN China Kennisnetwerk
UPT Erasmus
ERASMUS CENTRE FOR URBAN, PORT AND TRANSPORT ECONOMICS
Clingendael
Netherlands Institute of International Relations

Port politics: Strategic autonomy and European ports

A case study on Chinese involvement

Xiaoxue Martin
Bart Kuipers
Frans-Paul van der Putten

Clingendael Report
September 2024

September 2024

Cover photo © DPA / Picture Alliance via Reuters Connect

The research for and production of this report has been conducted within the framework agreement for the **China Knowledge Network (CKN)**. The aim of CKN is to promote strategic knowledge development about China for the national government of the Netherlands. Responsibility for the contents and for the opinions expressed rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the secretariat of the China Knowledge Network and/or the Netherlands Ministry of Infrastructure and Water Management and the Ministry of Foreign Affairs.

About the Clingendael Institute

The Netherlands Institute of International Relations 'Clingendael' is a leading think tank and academy on international affairs. Through our analyses, training and public platform activities we aim to inspire and equip governments, businesses, and civil society to contribute to a secure, sustainable and just world.

The Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Follow us on social media
@clingendaelorg
The Clingendael Institute
The Clingendael Institute
clingendael_institute
Clingendael Institute

Email: info@clingendael.org
Website: www.clingendael.org

About the authors

Xiaoxue Martin is Research Fellow at the Clingendael China Centre. Her work focuses on the contemporary politics and international relations of China, in particular Taiwan affairs, and China's relations with the United States and the European Union. She has researched topics including European dependence on China and Chinese influence in Europe's logistic sectors.

Bart Kuipers is Senior Researcher in Port Economics at Erasmus UPT. He focuses on the following research areas: freight transport, international and national regional-economic development related to freight transport, and freight transport policy and port policy.

Frans-Paul van der Putten is Senior Research Associate at the Clingendael Institute and founder of ChinaGeopolitics. His area of expertise is China's geopolitical role. He is the author of 'De Wederopstanding van China: Van prooi tot wereldmacht' (The Resurrection of China: A geopolitical history of China from 1840).

The authors would like to thank Anniek Sienot, Celine Leurs, and Tobias Koster for their contributions to this report.

Contents

Executive summary

European seaports and related logistics are a key part of international trade and logistics. In recent years, foreign involvement by third countries has gained greater significance in this sector, especially where China is concerned. The recent calls for a European port strategy in the European Parliament underline this. Individual Member States and the EU as a whole can actively influence future scenarios by managing the degree of foreign involvement in European seaports and logistics, with special attention for China's influence. However, a lack of EU cooperation concerning foreign involvement negatively impacts the EU's strategic autonomy. This limits control over future scenarios. **The aim of this report is therefore to conceptualise an EU-wide policy framework for strengthening strategic autonomy in the domain of seaports and related logistics sector systems. China serves as a case study.**

This draft strategic framework is designed as a building block for a country-agnostic policy framework. It should serve as a strategic tool, encompassing current and future European policies and instruments relevant to foreign influence in maritime infrastructure and related logistics. It brings added value by improving the current toolbox of instruments and promoting its implementation in the different EU Member States. A sector-specific approach can help create an overview of the internal connections and dynamics of a highly diverse and complex sector. This approach moreover goes beyond risk reduction of foreign involvement to also contribute to factors like economic competitiveness.

To build a common European approach, a strategic framework needs to strike a balance between national interests and the interests of the EU as a whole, as well as between economic integration versus economic security. It also needs to manage the different positions and views held by the Member States. This report finds that countries with seaports can be divided into the following groups:

a. Countries like Poland, Belgium and the Netherlands, which regard foreign involvement as a potential security threat that is urgent and requires coordination with other EU Member States or with the EU as a whole.
b. Countries like Germany and France, which regard foreign involvement as a potential security threat but seem to prefer to address this at the national level.
c. Countries like Italy, Spain, and Greece, which do not view foreign involvement in seaports and related logistics as a major security issue, or as the most important issue.

The concerns of all three categories of countries need to be considered for the framework to mobilise support. It is important that it helps the EU to de-risk from countries like China, minimising the related risks of foreign benefits while maximising the (economic) benefits.

In the light of these concerns, this report conceptualises a draft strategic framework based on the maritime logistics hub function, which is defined by four segments:

1. Port and maritime operations and infrastructures
2. Hinterland operations and infrastructures
3. Logistics support activities and infrastructures
4. Regional impact of logistics operations: warehouses/re-export operations

This report assesses the hardware, orgware and software of each segment, resulting in the overviews at the end of this executive summary (Figure 2 and Figure 3 in the report). The segments of the maritime logistics hub function and the three levels of hardware, orgware, and software in which this function is expressed, are used to identify risks to European strategic autonomy. Risk levels in the port and maritime infrastructures and the software domain are assessed as highest, including a serious risk to data disruption and therefore to strategic autonomy. Further research is needed into some elements with missing information, such as AI developments in deep-sea ports and maritime networks.

The draft strategic framework needs to be developed further with the EU and its Member States in order to be realised and implemented. While there are potential obstacles to the implementation of the draft framework, such as fears that it would undermine European competitiveness, there are also windows of opportunity like the European Parliament's calls for more strategic coordination concerning seaports.

In recent years the Dutch government has taken the lead in these efforts, meeting with the European Commission's Directorate-General Mobility and Transport (DG Move) and several Member States. This process needs to be continued to build support for a strategic framework, focusing first on building a coalition of interested Member States before jointly lobbying at the EU-level. The most logical countries to prioritise are those in category (a). While this will not be an easy process, it is essential if the EU truly wants to protect and strengthen its strategic autonomy.

Overview 1 Draft strategic framework: maritime logistics hub function

	Hardware	Software	Orgware
Port and maritime operations and infrastructures	– Investment in deep-sea terminals and additional port infra-structures – Ownership of land and port infrastructure – Computer hardware: IT-systems for terminal operations – Ships and other trans-port infrastructure and resulting cargo volumes	– Deep-sea terminal automation software – Port Community systems – Hinterland distribution software – AI-models/algorithms	– Efficient and uninter-rupted functioning of trade, logistical and transport processes – Level playing field and reciprocity in competition with third countries – Fair logistical practices according to legal, transparency, environmental and labour standards
Hinterland operations and infrastructures	– Investment in hinter-land terminals – Investment in trans-port infrastructure – Ownership of land – Computer hardware: IT-systems for terminal operations – Ships and other trans-port infrastructure and resulting cargo volumes	– Inland terminal auto-mation software – Port Community systems – Hinterland distribution software – AI-models/algorithms	– Efficient and uninter-rupted functioning of trade, logistical and transport processes – Level playing field and reciprocity in competition with third countries – Fair logistical practices according to legal, transparency, environmental and labour standards
Logistics support operations and infrastructures	– Office functions in seaports and large hinterland nodes for i.a. finance, legal, insurance, risk-development, strategy functions – Part of port-innovation ecosystem/knowledge infrastructure	– Port Community systems – AI-models/algorithms – Port innovation eco-systems – Financial transaction software	– Level playing field and reciprocity in competition with third countries – Fair practices according to legal, transparency, environmental and labour standards
Regional impact of logistical operations	– Warehouses in port and hinterland	– Warehouse software – AI-models/algorithms – Distribution software	– Level playing field and reciprocity in competition with third countries – Fair logistical practices according to legal, transparency, environmental and labour standards

Overview 2 Draft strategic framework: potential risks posed by foreign involvement to strategic autonomy of EU-ports and related logistics

	Hardware	Software	Orgware
Risk levels to strategic autonomy	No risk Limited risk: market share <10% Some risk: share 10-25% Serious risk: market share 25-50% Very serious risk: share >50%	No risk Limited risk to data disruption Some risk to data disruption Serious risk to data disruption Very serious risk to data disruption	No risk Limited risk strategic autonomy Some risk to strategic autonomy Serious risk to strategic autonomy Very serious risk to strategic autonomy
Port & maritime operations and infrastructures	**Deep-sea terminals:** – High dependency on logistics, trade and investment strategies of third countries due to high market share – Dual use of terminals for commercial and military purposes **Ownership port infrastructure/ authority:** – Decision-making power shifting to third countries through high share of ownership **Computer hardware:** – Use of suppliers of third countries at the expense of local firms – Legacy systems **Cargo volumes:** – Vulnerability to trade sanctions and geopolitical risks associated with conflicts with third countries. Potential negative effects on port employment/added value creation	**Deep-sea terminal systems:** – Legacy systems – Vulnerability to cyber-attacks – Third-country suppliers of IT-hard-ware and software – Vulnerability through modems or wireless transmitters of sys-tems that are not connected to internet – Low data-hygiene personnel **Port Community systems:** – Concentration of data in one system – All information is processed, including sensitive/military data – Differences in security demands in port com-munity systems in EU **AI-models/algorithms:** – Strategic sensitivity analyses, manipula-tion strategies and forecasts produced by third countries – Further research needed	**Efficient and uninterrupted functioning of trade:** – Lack of organisational measures in ports to increase cyber resilience – Low awareness and understanding of cyber threats **Level playing field and reciprocity:** – No level playing field or reciprocity by third countries (e.g. inter-national relay) – Strong home market advantages by third countries – Preferential treatment of third countries when selecting sub-contractors – Low environmental concern in the realisa-tion of investment by third countries **Fair logistical practices:** – See above – Strong political pres-sure influencing busi-ness deals by SOEs of third countries – Coercion of EU-service providers to use local service providers when exporting to third countries

Hinterland operations and infrastructures	**Hinterland terminals and intermodal networks:** – See above – Intermodal corridor development-strategies by third countries **Ownership port infra/ authorities:** – See above **Computer hardware:** – See above **Cargo volumes:** – Intermodal cargo volumes driven by seaport volumes (see above)	**Inland terminal systems:** – Hinterland terminals increasingly connected to seaports via port community systems, systems of carriers, forwarders, etc. – Vulnerability of hinterland infrastructure because of legacy systems or lack of maintenance – Data-hygiene SMEs at lower level **Port Community systems:** – See above **AI-models/algorithms:** – See above	**Efficient and uninterrupted functioning of trade:** – Lack of organisational measures in inland ports to increase cyber resilience – Low awareness and understanding of cyber threats **Level playing field and reciprocity:** – See above **Fair logistical practices:** – See above
Logistics support operations and infrastructures	**Port-related office functions:** – Leak of sensitive information when assessing port business networks **Port-innovation ecosystem:** – Increased foreign influence or data leakage through participation of SOEs from third countries – Knowledge security risks in sensitive research areas through PhD-candidates or students of military universities from third countries	**Port-related office functions:** – Leak of sensitive information in assessing port business networks **Port-innovation ecosystem:** – Increased foreign influence or data leakage through participation of SOEs by third countries – Knowledge security risks in sensitive research areas through PhD-candidates or students of military universities from third countries	**Efficient and uninterrupted functioning of trade:** – Lack of organisational measures in logistics support operations to increase cyber resilience – Low awareness and understanding of cyber threats **Level playing field and reciprocity:** – See above **Fair logistical practices:** – See above
Regional impact of logistical operations	**Warehouse districts:** – Trade disputes or geopolitical tensions with third countries impacting employment or added value creation	**Warehouse districts:** – Risks are limited through decentralised organisation and a large number of different organisations – There are some large e-commerce providers from China with operations (JD, Alibaba), but a minority share	**Efficient and uninterrupted functioning of trade:** – Lack of organisational measures in warehouse organisations or districts to increase cyber resilience – Low awareness and understanding of cyber threats **Level playing field and reciprocity:** – See above **Fair logistical practices:** – See above

Source: expert interviews. Note: not an exhaustive enumeration but demonstrative of the functioning of the strategic framework.

1 Introduction

This chapter introduces the research aim of this report: to conceptualise an EU-wide policy framework for strengthening strategic autonomy in the domain of seaports and related logistics sector systems. It also formulates the research questions this report seeks to answer. The chapter then discusses why China serves as a case study for the research, explains the need for a strategic policy framework and describes the research methodology. Lastly, it provides an overview of the report chapters.

1.1 Research aim

European seaports and related logistics are a key part of international trade and logistics.[1] In recent years, foreign involvement by third countries has gained greater significance in this sector.[2] This trend is driven by the growing geopolitical instability and by governments' increasing willingness to use economic tools to exert influence abroad. An important actor in this regard is China. Chinese companies, many of them state-owned, have become major players in multiple European seaports and throughout the logistics system that connects the EU with the rest of the world.[3] They facilitate trade, provide investments, and supply European ports and logistics companies with equipment and technology. While this has economic benefits for the EU, it has also turned China into an influential actor in European maritime logistics.

1 This study was conducted on behalf of the Dutch Ministry of Infrastructure and Water Management and the Ministry of Foreign Affairs, within the framework agreement for the Dutch China Knowledge Network (CKN).

2 Foreign involvement relates to the involvement of non-EU actors in maritime infrastructure or related logistics in the EU, or in activities outside the EU that play a significant role in relation to the functioning of EU maritime infrastructure or related logistics.

3 For the purpose of this study, references to 'China' and 'Chinese' include Hong Kong unless specified otherwise, though we acknowledge that there are important differences between companies based in mainland China and those based in the People's Republic of China's Special Administrative Region Hong Kong. These differences are discussed in e.g. "China's Strategic Relevance for the Port of Rotterdam", Clingendael Report, December 2023.

European seaports and related logistics impact the EU's strategic autonomy, which this study understands as the EU's capacity to act independently of foreign governments in strategically important policy areas, such as national economic competitiveness, national security, and geopolitical positioning.[4] Strengthening strategic autonomy has become a key goal of European policymakers. However, European seaports and EU Member States compete among each other to attract trade and investments, which limits the EU's ability to protect its strategic autonomy. In addition, there is the possibility that foreign governments increasingly influence the channels through which goods enter and leave the EU. Other concerns are linked to the ability of seaports to operate without interruptions and to the integrity of sensitive data.

Ideally, foreign involvement is managed in a way that protects European strategic autonomy and contributes to an efficient and competitive port and logistics system. For this, cooperation between the EU and its Member States is necessary. **The aim of this report is therefore to conceptualise an EU-wide policy framework for strengthening strategic autonomy in the domain of seaports and related logistics sector systems.**

In addition to conceptualising a strategic framework, this report also addresses the following **questions**:

1. This report builds on the research of a previous report by the authors, '*Navigating an Uncertain Future*'.[5] To what extent can the Dutch government or the EU actively influence the likelihood and direction of the scenarios mentioned in the previous report, instead of merely reacting to them?
2. How can the proposed strategic policy framework help bridge differences in the positions and interests held by EU Member States in relation to foreign involvement in seaports and related logistics?
3. Which policy instruments are needed, both at EU and Member State level, in order to enable European authorities to align foreign involvement in European seaports and related logistics with the goal of strategic autonomy? What is already addressed by existing instruments?

4 EU Strategic Autonomy Monitor, "EU Strategic Autonomy 2013-2023", July 2022.

5 Frans-Paul van der Putten, Xiaoxue Martin & Bart Kuipers, "Navigating an Uncertain Future", Clingendael Report, November 2022.

1.2 The case of China

The draft framework presented in this report is based on an analysis of the role of China in European seaports and related logistics. The country serves as a case study partly because this report is a follow-up to the previously mentioned China-focused research '*Navigating an Uncertain Future*', but more importantly because of China's unique economic and geopolitical impact. The EU sees China not only as a partner for cooperation, but also as an economic competitor and a systemic rival.[6] Chinese companies currently constitute the largest single group of non-EU actors in EU seaports in terms of value of direct investments, and are also significant as shipping companies.

While this report takes Chinese involvement as a case study, the resulting draft framework is intentionally designed as a building block for a country-agnostic policy framework. This would be in line with the EU's country-agnostic approach to policymaking. This design also acknowledges that, aside from China, there are many other non-EU countries whose companies or investors play a role in the (future of) EU's seaports and related logistical activities. Concerns related to strategic autonomy exist not only in relation to China. Additional analyses of other relevant actors would strengthen the creation of a generic framework to address foreign involvement regardless of any specific country origin. Therefore, a country-agnostic policy framework is most suitable to provide the foundation for a European strategy for seaports and port-related logistics.

Finally, the focus on China as a case study is not meant to imply that Chinese or other foreign commercial involvement in the EU and EU-China economic relations should be avoided altogether. Rather, this report fits in the EU's push for de-risking under President Von der Leyen, and argues that a policy framework is necessary to maximise the economic benefits of foreign involvement while managing the related risks.

6 European External Action Service, "EU-China Relations Factsheet", December 2023.

1.3 The need for a strategic policy framework

The purpose of the draft policy framework in this report is to bring together European policies relevant to managing foreign involvement in seaports and related logistics. Its main objective is to support policymakers in the EU – within the Member States and at the Union level – in addressing foreign involvement in such a way that it aligns with the aim of strengthening European strategic autonomy. The framework focuses on protecting market forces in the maritime logistics sector where this is possible, without weakening Europe's strategic autonomy.

The conceptualisation of a strategic framework was a recommendation of a previous study by the Clingendael Institute and Erasmus UPT, '*Navigating an Uncertain Future: An exploration of China's influence on the Netherlands' future maritime logistics hub function*' (2022).[7] That report conducted a scenario study and indicated that the Dutch government should prepare for difficult dilemmas arising from the importance of economic cooperation with China, combined with the need to maintain strategic room to manoeuvre and protect Dutch security interests. The report therefore recommended that the Dutch government should take an active approach and work towards an EU-wide strategic policy framework for foreign involvement in seaports and related logistics.

The present report is based on the premise that it is important for the EU to develop a strategic approach specifically for seaports and port-related logistics. There are two main benefits to such a **sector-specific approach**. The first is that it makes it possible to create an **overview of the internal connections and dynamics** of a highly diverse and complex set of actors, technologies, markets, industries and processes, both within and outside the EU. For instance, in the case of China, relevant factors include the position of Chinese companies in global shipping alliances, Chinese involvement in infrastructure, logistics and digital port community platforms in Africa, Latin America and Asia, hinterland logistics in the EU, EU access to related sectors in China, China's government policies and its relations with major powers, and China's role in global trade, shipbuilding, maritime finance and insurance, and manufacturing of port equipment.

7 Frans-Paul van der Putten, Xiaoxue Martin & Bart Kuipers, "Navigating an Uncertain Future", Clingendael Report, November 2022.

The second benefit of a sector-specific strategic framework is that it allows for an **approach that goes beyond risk reduction of foreign involvement**. Even though risk reduction would be a major goal of the strategic framework, it should also contribute to greater economic competitiveness. The main alternative currently available is the EU's Economic Security Strategy, the outline for which was published in June 2023.[8] It consists of three main components, or pillars. The 'protect' pillar specifically aims to prevent or reduce economic security risks. The 'promote' pillar aims to make the EU more competitive by investing in European capacities and diversifying its supply chains. In other words, the aim is not to strengthen economic competitiveness as such, but to do so in regard to certain security vulnerabilities by lessening dependence on external actors. Finally, the 'partnering' pillar is directed at increasing cooperation with non-EU actors, but only with those 'who share our concerns on economic security as well as those who have common interests and are willing to cooperate with us to achieve the transition to a more resilient and secure economy'.

Although no country is mentioned by name, it seems clear that China – despite being the world's largest manufacturing and trading nation and the third-largest consumer market – is among the countries that are largely excluded from this approach. So in this regard, too, the emphasis of the Economic Security Strategy is on reducing risks rather than striking a balance between minimising risks and maximising economic competitiveness. Chapter 3 will elaborate on the current EU instrument toolbox.

A distinct strategic approach for seaports and port-related logistics would be an important complement to the EU Economic Security Strategy and to the EU policy tools discussed later in this report. It would allow for an effective way to address security risks, because it would be tailored specifically to a highly diverse sector that includes many actors and processes outside Europe. At the same time, it would be more effective in balancing security and economic interests than an Economic Security Strategy could.

8 European Commission, "Joint Communication to the European Parliament, the European Council and the Council: On European Economic Security Strategy", Juni 2023.

1.4 Research methodology

To answer the research questions listed in section 1.1, this report takes into account the positions of eight Member States: Belgium, France, Germany, Greece, Italy, the Netherlands, Poland, and Spain. These countries were chosen for their relevance to European seaports and related logistics, and their diverse geographic positions.

This study is based on extensive **interviews and consultation sessions** with experts, policymakers, and sector representatives from the eight Member States, as well as with the European Commission's DG Move. The interviewee list can be found in the Appendix. It is also based on **desk research** of publicly available information.

1.5 Report overview

- Chapter 2: describes the types of foreign involvement, China's role, and key dilemmas in foreign involvement in European maritime logistics and infrastructure.
- Chapter 3: provides an overview of the current toolbox of relevant policy instruments, both at the EU level and within the eight EU Member States. Next, it explains how a strategic framework could bring added value to the toolbox, helping to utilise it more effectively and to encourage Member States to implement the available instruments.
- Chapter 4: outlines the main functions of a strategic framework and conceptualises a draft design. It uses four segments of the maritime logistics hub function, and subsequently discusses hardware, orgware and software for each level.
- Chapter 5: uses the draft framework to assess risks to strategic autonomy related to foreign involvement. It shows that risks are highest in the software domain, and details how existing EU instruments relate to the risks.
- Chapter 6: outlines the steps towards further developing and implementing a strategic framework. It lists obstacles as well as windows of opportunity for the realisation of a framework.
- Chapter 7: offers conclusions and recommendations based on the findings of the previous chapters.
- Appendices: list this report's interviewees and give a more detailed overview of EU instruments.

2 Chinese involvement in European seaports and port-related logistics

This chapter outlines the international context relevant to foreign involvement in European seaports and related logistics. It discusses the different types of foreign involvement, as well as China's role in seaports and the related logistical sector. Key issues are highlighted by discussing the different economic interests and risk perceptions across Member States.

2.1 Types of foreign involvement

The EU has become increasingly concerned about **security risks** resulting from its economic relations with third countries, including China. Types of involvement by companies or technologies from outside the EU in seaports and related logistical sectors include:

- **Direct investments**, either through acquiring substantial shares in or full ownership of EU-based companies such as port or terminal operators, transport firms, or storage providers.
- **Vertical integration**, established through organic growth, direct investments, strategic alliances, or a combination thereof.
- **Land ownership or leases of land-use** in ports or in port-related areas, either through direct investments in EU companies or by land purchases or long-term leases.
- Involvement in **port operating, communication, or data systems**, either as commercial users of a port or as providers of equipment, software, port data platforms, or technological services.

The EU has taken steps to expand its toolbox to manage these types of involvement, such as stricter investment screening, which will be discussed in Chapter 3.

2.2 The role of China

The increased European focus on security risks in its economic relationship with China is driven by several developments:

1. China has become a leading economic power and a major competitor to the EU, and has become more active on the international stage. Indicators of this include China surpassing Japan as the world´s second-largest economy in 2010, a rapid surge in direct investments in the EU from 2010-2017, and China becoming a major lender to many developing countries. In 2013 China launched its Belt and Road Initiative (BRI), aimed at strengthening economic ties with Europe, Russia and developing countries in Asia, Africa, and Latin America. As a consequence of this approach, Chinese interests in transport infrastructure and logistics in many parts of the world, including in the EU, increased rapidly. Despite the current slowdown of China's economic growth, the country remains a major economic actor. In 2023, China was still the largest source of goods imported into the EU, and the third-largest destination of goods from the EU, behind the US and the UK.[9]
2. China has a state-driven economic model. Combined with China's large economic size, this has caused concerns in the EU that the European more liberal and open economic model is vulnerable in the face of Chinese companies that benefit from state aid and other asymmetric advantages.
3. The power struggle between the US and China has a major effect on the EU's relations with China. The US government is increasingly pressuring European governments and companies to decrease their economic and technological interactions with Chinese counterparts. The US appears to want to slow down China's emergence as a technological, military and economic world power, to limit Europe's economic dependence on China, and to strengthen the role of European allies in security matters relating to China. At the same time, the Chinese government aims to build and maintain close economic and technological ties with the EU, and to weaken Europe's alignment with the US' geopolitical position.
4. The Russian invasion of Ukraine in 2022 revealed the close strategic relationship between China and Russia and its relevance for European security. China's enduring ties with Russia undermine the effectiveness of EU sanctions aimed at forcing Russia to withdraw from Ukraine.

9 Eurostat, "Principal Partners for EU Exports of Goods", 2023.

Moreover, two recent instances of Chinese direct investment in EU seaports attracted much attention from European media and governments: COSCO's purchase in 2016 of a majority stake in the **Piraeus Port Authority**, and in 2023 COSCO's purchase of a minority stake in a container terminal in the port of **Hamburg**. These cases focused attention on the dilemmas concerning Chinese investments and intensified the policy debate. Moreover, the cases showed the lack of a common European approach towards foreign involvement, despite the broader consequences of the investments for the European sector as a whole.

2.3 Key issues

Through conversations with the interviewees listed in the Appendix as well as through desk research, the following key issues emerged in relation to the building of a common European approach to addressing Chinese involvement in ports and related logistics.

National versus common EU interests

A dilemma that exists at the level of the EU Member States is how to strike **a balance** between protecting national interests and strengthening the EU's ability to confront major powers such as China. Even the largest economies in the EU are, when considered individually, small compared to China. However, the EU as a whole is one of the leading economic actors globally and can operate on a more level playing field with China. In the domain of seaports and related logistics, a common EU strategy would greatly contribute to the goal of minimising the risks and maximising the benefits of China's involvement in the sector. **A joint approach would reduce the potential for foreign actors to pit their European counterparts against each other.**

Investment screening is an example of a related policy area in which the EU has made progress in recent years, despite the tension between national and common EU interests. Although the EU has no centralised screening mechanism, it did adopt a common framework for national investment screening in 2020. Such an approach aimed to improve the EU's bargaining position and help it attain more favourable economic outcomes from foreign investments, including from China. It would also reduce the risk that the Chinese government could control the EU's external trade flows.

Different positions and views among Member States

The initial assessment for this report suggests that there are **major differences** among Member States in at least the following respects.

- Seaports: not all Member States have seaports. An EU-wide approach would need to distinguish between coastal countries and landlocked countries.
- Risk perception: not all coastal Member States regard Chinese involvement in seaports or related logistics as a significant issue, or as a more important issue than economic competitiveness. The main distinction in this regard seems to be between southern and northern Member States.
- Sense of urgency linked to a need for EU-wide action: among the coastal countries that do have security concerns regarding Chinese involvement in ports and logistics, the sense of urgency to act at the EU level can vary. The main distinction here appears to be between larger and smaller Member States. The larger countries may have a greater ability to address unwanted Chinese involvement at the national level. They may also feel less urgency because their economy depends less on their individual ports.

The countries studied for this report – all of which have major seaports – can be divided into **three groups**:

a. Poland, Belgium and the Netherlands regard foreign involvement as a potential security threat that is urgent and requires coordination with other EU Member States or with the EU as a whole.
b. Germany and France regard foreign involvement as a potential security threat, but seem to prefer to address this at the national level.
c. Italy, Spain and Greece do not view foreign involvement in seaports and related logistics as a major security issue, or as the most important issue.

Government regulation versus market forces

The EU has long favoured an open economic system and a limited role of governments in international economic relations. However, EU Member States and the European Commission have become more active in shaping the behaviour of companies and markets, given the relatively high degree of state involvement in China's economy and the rapidly increasing politicisation of international economic relations due to geopolitical rivalry. Relevant policies are driven by the aim of strengthening the EU's strategic autonomy by reducing economic security risks and improving economic competitiveness. How far should European governments expand their role in economic affairs before the effort to preserve market forces turns into a strategy of protectionism?

This question goes beyond finding the right balance between **security and economic interests**. In the domain of seaports and logistics it also involves deciding how much **concentration of economic power** is desirable, e.g. in terms of shipping alliances or in vertical integration, regardless of the nationality of the companies involved.

Economic integration versus economic security

Addressing economic security concerns has become a priority for the EU. This development raises the question how to combine the aim of reducing security risks with the aim of **continuing economic relations with China**. Economic interaction with China can benefit the EU economically, and economic power is the main source of EU influence internationally. For the EU to strengthen its strategic autonomy it must limit economic security risks, but also continue economic relations with China. How far, then, can the EU take the process of de-risking economic ties with China before it becomes counterproductive? Or put differently, given that risk is an inherent part of economic interaction with China, what level of risk is acceptable? And how does this dilemma relate to maritime logistics and infrastructure?

Potential risks of the involvement of Chinese companies in EU seaports and logistics include:

- That the Chinese government acquires so much influence over the EU's external trade flows that it can use this to **limit** the EU's access to foreign markets, disrupt its supply chains, diminish the EU's competitive strength, coerce or manipulate the EU or its Member States on specific issues, or undermine EU or NATO unity.
- That the involvement of Chinese companies or their products or services in EU ports allows the Chinese government to **disrupt** the functioning of those ports, gain access to strategically important logistical data, or leverage their dependence on Chinese technology for political or competitive purposes.
- That the involvement of Chinese companies or their products or services in EU ports allows the **Chinese state to gain easier access** to these ports for military intelligence gathering.

Potential benefits of the involvement of Chinese companies in EU seaports and logistics include:

- A greater likelihood that EU companies can **maintain their investments** and keep investing in China's seaports and logistics.
- A degree of **mutual dependence** that increases the cost for the Chinese government to act against the interests of the EU.
- Increased **access** to Chinese capital and/or technology for EU companies in maritime logistics, and a greater likelihood of Chinese logistical companies using EU rather than non-EU ports as main hubs.
- A greater potential to **diversify** sources of foreign involvement in EU maritime logistics.
- In some cases, Chinese involvement could lead to a greater **resilience** of Europe's external transport corridors. A recent example of this were COSCO's efforts to set up a rail connection between Zeebrugge and Central Europe. Due to the recent attacks on international shipping by Yemen's Houthis, many ships on Asia-Europe lines have been rerouted via South Africa and no longer service Piraeus but instead go straight to Europe's northwestern ports. COSCO has responded by servicing Central Europe via Zeebrugge instead of Piraeus, as the company has major investments – and thus interests – in both ports.[10]

There are several considerations when weighing the listed risks and benefits. First, not all of the above-mentioned risks are equally relevant or imminent. But if they are conceivable, they must be considered. Second, the potential benefits are also not guaranteed. Optimisation of benefits requires greater European coordination. Third, it matters substantively whether or not the EU and its Member States regard China as a possible military adversary, in the next decades or sooner. The more China is perceived as an imminent threat, the heavier the risk side weighs, while the benefits lose some of their relevance.

The latter mainly relates to the possibility of a Sino-American conflict in Asia combined with the chances of EU Member States becoming involved in such a conflict. Another scenario is that the EU starts considering China as a military ally of Russia, and thus as a direct and imminent threat to European security. Then, China's economic involvement in European ports and maritime logistics could involve risks relating to Russia as a military threat. Although strategic

10 RailFreight.com, "Lineas Sets Up New Route", February 2024.

cooperation between China and Russia has been increasing since the late 1990s, the two powers are not tied to each other through a formal military alliance. However, there have been calls among European experts to label China as a security threat to Europe.[11]

While geopolitical uncertainty has become a major feature of international affairs, it is important that European authorities carefully assess the likelihood and relevance of various scenarios and consider where and to what degree the EU can influence geopolitical processes.

11 Natalie Sabanadze, Abigaël Vasselier & Gunnar Wiegand, "China-Russia Allignment: a Threat to Europe's Security", MERICS, Chatham House and GMF Report, June 2024.

3 The European toolbox of policy instruments

This chapter discusses the current toolbox of policy instruments relevant to foreign involvement in European seaports and related logistics, considering the issues discussed in the previous chapter. It first provides an overview of existing instruments at the EU level, as well as within eight EU Member States: Belgium, France, Germany, Greece, Italy, the Netherlands, Poland, and Spain. Then, it explains how a strategic framework could bring added value to the toolbox, helping to utilise it more effectively and encouraging Member States to implement the available instruments.

3.1 Existing EU instruments

The EU has taken steps in recent years, introducing several instruments that aim to better protect the EU and its Member States in a more complex geopolitical environment. These are also relevant to the issues and dilemmas discussed in the previous chapter. At the time of writing, the EU has the following toolbox to manage foreign involvement in seaports and logistics:

Table 1 EU instruments relevant to foreign involvement in European seaports and logistics

Instrument	Status
Economic Security Strategy[12]	24 January 2024: EC adoption of five initiatives to strengthen economic security.
EU framework for foreign direct investment screening (Regulation 2019/452)[13]	24 January 2024: EC proposal for a revision.
Directive on the Resilience of Critical Entities (CER) (Directive (EU) 2022/2557)[14]	18 October 2024: application of the regulation (planned).
Network and Information Directive (NIS2) (Directive (EU) 2022/2555)[15]	18 October 2024: application of the regulation (planned).
Foreign subsidies Regulation (FSR) (Regulation (EU) 2022/2560)[16]	12 July 2023: application of the regulation.
Anti-Coercion Instrument (ACI) (Regulation (EU) 2023/2675)[17]	27 December 2023: instrument entered into force.
Consortia Block Exemption Regulation (CBER) (Regulation (EC) 906/2009)[18]	25 April 2024: expiration CBER, after which consortia are subject to the EU antitrust rules that apply to all economic sectors.
Horizontal Co-operation Agreement (OJ C 11)[19]	21 July 2023: Revised Horizontal Guidelines.
Revision of TEN-T Regulation 2013 (2021/0420(COD))[20]	June 2024: entered into force.

12 European Commission, "An EU approach to enhance economic security", June 2023.
13 European Commission, "EU Framework for Investment Screening".
14 The European Parliament and the Council of the European Union, "On the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC", December 2022.
15 The European Parliament and the Council of the European Union, "On Measures for a High Common Level of Cybersecurity Across the European Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)", December 2022.
16 The European Parliament and the Council of the European Union, "On Foreign Subsidies Distorting the Internal Market", December 2022.
17 The European Parliament and the Council of the European Union, "On the Protection of the Union and its Member States from Economic Coercion by Third Countries", November 2023.
18 The Commission of the European Communities, "On the Application of Article 81(3) of the Treaty to Certain Categories of Agreements, Decisions and Concerted Practices between Liner Shipping Companies (Consortia)", September 2009.
19 European Commission, "Horizontal Co-operation Agreement (OJ C 11)", January 2011.
20 European Commission, "Regulation of the European Parliament and of the Council: on Union Guidelines for the Development of Trans-European Transport Networks, Amending Regulations (EU) 2021/1153 and Regulation (EU) No 913/2010 and repealing Regulation (EU) 1315/2013", December 2021.

Instrument	Status
European Ports Alliance[21]	24 January 2024: launched by the European Commission, during the Belgian Presidency of the Council of the EU.
Revised EU Maritime Security Strategy (EUMSS)[22]	24 October 2023: approved by the Council of the EU.
AI Act (Regulation (EU) 2024/1689[23]	1 August 2024: regulation entered into force. August 2026: rules will apply on "high risk" AI systems, including critical infrastructure.

A more detailed discussion of the objectives, relevant features, and status of these instruments listed in Table 1 can be found in Appendix B.

3.2 Existing instruments within EU Member States

EU Member States have different positions and risk perceptions. This explains the differences in existing national instruments among the Member States. They have widely varying policy approaches towards seaports and logistics and deal with different levels of foreign involvement. This is highlighted in Table 2 and Table 3. Crucially, Member States have different definitions for 'critical infrastructure' and 'provider of critical infrastructure', and some do not have a clear definition at all. This means that Member States do not apply their investment screening regime to seaports and logistics in the same way. Greece, for instance, doesn't yet have an investment screening regime, although it did implement a law to attract large-scale investments in 2019.

21 European Commission, "European Ports Alliance", January 2024.

22 European Commission, "Maritime Security Strategy", October 2023.

23 European Commission, "Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)", June 2024.

Table 2 EU Member States and foreign involvement instruments

	Chinese investments in container terminals	FDI screening mechanism	Proactive approach to EU-policy[24]	Other relevant policy instruments
Belgium	COSCO, China Merchant Port Holdings, Hutchison Port Holdings. Majority and controlling stakes.	Yes	No	Maritime Security Act (2023).
France	China Merchants Port Holdings. Minority stakes.	Yes	No	Critical Information Infrastructure Protection Law (2013).[25]
Germany	COSCO and Hutchison Port Holdings. Minority stakes.	Yes	No	National Strategy for Critical infrastructure protection (2009).[26]
Greece	COSCO, China Merchant Port Holdings. Majority stakes and operational control of Piraeus port authority.	No	No	Strategic Investment Law (2019).[27]
Italy	COSCO, Qingdao Port International Development.	Yes	No	
The Netherlands	COSCO Shipping, Hutchison Ports, Hutchison Ports Holdings. Minority stakes.	Yes	Yes	Security of Network and Information Systems Act (2018)[28] Aanpak vitaal 2023-2028.[29] Beschermingsvoorziening Economische Veiligheid (2023).[30]
Poland	Hutchison Port Holdings.	Yes	Yes	
Spain	COSCO, Hutchison Port Holdings. Controlling stake and minority stakes.	Yes	No	Law 8/2011 (2011).[31]

24 This category describes whether the Member State has a proactive approach towards formulating EU-level policy concerning foreign influence in maritime infrastructure and logistics. It is based on the desk research and expert interviews conducted as part of this study from 2023 to February 2024.

25 French General Secretariat for Defence and National Security, "French Critical Infrastructure Protection Framework", accessed August 2024.

26 German Federal Ministry of the Interior and Community, "Critical Infrastructure Protection in Germany", accessed August 2024.

27 United Nations Conference on Trade and Development, "Strategic Investment Law", April 2019.

28 The Netherlands National Coordinator for Security and Counterterrorism [Nationaal Coördinator Terrorismebestrijding], "Wet Beveiliging Netwerk- en Informatiesystemen", November 2018.

29 The Netherlands National Coordinator for Security and Counterterrorism [Nationaal Coördinator Terrorismebestrijding] "Aanpak Vitaal 2023-2028", April 2023.

30 The Netherlands Ministry of Economic Affairs and Climate [Ministerie van Economische Zaken en Klimaat], "Uitwerking Beschermingsvoorziening Economische Veiligheid en Overzicht Instrumentarium Economische Veiligheid", September 2023.

31 Official Gazette of the Kingdom of Spain [Boletín Oficial del Estado], "Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas", April 2011.

Table 3 EU Member States and FDI screening

	FDI screening mechanism	Scope
Belgium	Current mechanism entered into force 1 July 2023 with retroactive application.[32]	– Applies to non-EU investors. – Trigger threshold 10% or 25% depending on the sector. – Includes critical infrastructure and providers of critical infrastructure.
France	Since 2014 Montebourg Decree.[33]	– Applies to non-French investors. – Trigger threshold 10% or 25% depending on the sector. – Includes 'essential' infrastructure.
Germany	Since 2004 German Foreign Trade and Payments Act/Ordinance.[34]	– Generally applies to non-EU investors, and to non-German investors for some sectors. – Threshold 10% for (software for) critical infrastructure.[35]
Italy	Since 2012 Decreto Legge (Golden Power).[36]	– Applies to EU and non-EU investors depending on the investment. – Trigger threshold 10%. – Includes critical infrastructure.
The Netherlands	Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo) entered into force 1 June 2023, with retroactive application.[37]	– Applies to all investors in the specified sectors. – Includes providers of 'vital' processes, including certain providers of port activities.
Poland	Since the Act of 2015 on the Control of Certain Investments.[38]	– Applies to all investors in the specified sectors. – Includes ports of major importance to the national economy.
Spain	Since Real Decreto 664 (Royal Decree) (1999).[39]	– Applies to non-EU investors and EU investors controlled by foreign investors. – Trigger threshold 5% or 10% depending on the sector. – Includes critical infrastructure.

32 Flanders Chancellery & Foreign Office [Departement Kanselarij en Buitenlandse Zaken], "Interfederal Foreign Investment Screening Mechanism", July 2023.

33 The French Ministry of Economics, Finance and Industrial and Digital Sovereignty [Ministère de L'Economie, Des Finances et de La Relance], "Foreign Direct Investment Screening in France", October 2023.

34 The Organisation for Economic Co-operation and Development, "Investment Data", accessed August 2024.

35 United Nations Conference on Trade and Development, "Germany Expands the Scope of its FDI Screening Regime", December 2018.

36 United Nations Conference on Trade and Development, "Decreto Legge", March 2012.

37 The Netherlands Ministry of Economic Affairs and Climate [Ministerie van Economische Zaken en Klimaat], "Wet Veiligheidstoets op Investeringen, Fusies en Overnames", June 2023.

38 Polish Government, "Act of 24 July 2015 on Control of Certain Investments. Dziennik Ustaw 2015, no. 1272", 2015.

39 United Nations Conference on Trade and Development, "Spain Extends and Expands the FDI Screening Regime until 31 December 2024", December 2022.

3.3 Improving and implementing the existing instrument toolbox

The EU and its Member States thus already have a selection of instruments that could be used to address foreign involvement in seaports and logistics. However, not all of the issues outlined in Chapter 2 are addressed. The implementation of the toolbox can furthermore be strengthened. At the moment, Member States unevenly implement or use the available instruments, due to their different viewpoints discussed in the previous chapter. There also needs to be a better coordination of the instruments to cover seaports and logistics. To truly protect European strategic autonomy, this report therefore proposes a coherent strategic policy framework specifically for seaports and related logistics.

Ongoing debates in the European Parliament and European Commission

Several of the instruments in Table 1 are currently under discussion in the EU, with both the European Commission and European Parliament suggesting ways to refine the toolbox. This provides a window of opportunity for the strategic framework conceptualised in this report. The **Commission** has proposed, among other things, a revision of the Regulation on the screening of FDI. It seeks to close gaps in the current mechanism, for instance by ensuring all EU Member States have a screening system, and by facilitating the convergence of national systems. The **European Parliament** is also pushing for further measures to protect European infrastructure. The Parliament argues that recent legislation is too focused on FDI screening, while other possible channels of foreign influence such as supply chain dependencies are left unaddressed. Moreover, it believes a risk assessment and mapping framework for critical infrastructure is necessary. Its concerns are in line with the worries noted by the people interviewed for this report.

On 17 January 2024, the European Parliament adopted a **resolution on China's influence in critical infrastructure** that referred to COSCO's investment in Hamburg, and that pointed at a link between Chinese investments in ports and visits by the Chinese navy. According to the European Parliament, such naval visits 'reveal areas of influence, prioritised operational zones, intelligence collection objectives and cooperation priorities'. The EP therefore 'considers it necessary to map, track and assess China's and other third countries' access to critical infrastructure in the EU and to jointly proceed with mitigating measures where necessary.'[40]

40 European Parliament, "European Parliament resolution of 17 January 2024 on the security and defence implications of China's influence on critical infrastructure in the European Union", January 2024

Another resolution, adopted on the same date and based on a report prepared by Member of Parliament Tom Berendsen, specifically addresses the need for building a **European port strategy**. In that resolution, the European Parliament calls on the Commission 'to present an EU strategic policy framework to reduce and limit the influence and financial and operational control exerted over the EU's ports and in their processes and hinterland operations by non-EU countries, including cases of participation and control in the management of a port authority, in the spirit of finding a balance between keeping an open investment environment and mitigating risks.'[41]

The European Commission has since responded to this resolution, listing its existing instruments and writing:

> "*The European Union has already taken strong action during the current mandate to strengthen competitiveness, security, resilience and the control of foreign influence in the European economy, including in ports [...] The Commission remains open to considering options for future action, if these are balanced [...] and can bring a clear value-added to existing strategies and tools without adding excessive additional administrative burden. However, any such new initiatives would be for the next Commission to decide.*"

The value-added of a strategic framework

A strategic framework could bring value-added to the existing instruments and promote a more effective use of the toolbox. It could address problems identified in the EP's resolutions by taking a **broad view** of seaports and logistics. First, it looks beyond individual Member States, recognising that an **overarching European approach** is needed. Foreign influence goes beyond country borders. It is the combined effect of Chinese investments that should be considered, rather than individual investments. These should be seen from an economic *and* a political point of view.

For individual ports, European strategic autonomy is not the main factor when considering foreign investments. However, a European approach could the Member States' different interests and approaches to seaports and logistics,

41 European Parliament, "European Parliament resolution of 17 January 2024 on building a comprehensive European port strategy", January 2024.

and help overcome competition between the ports in the EU. A framework can provide added value here, by ensuring that ports do not accept greater foreign involvement in order to increase their competitiveness vis-à-vis other European ports – as was a consideration of the Port of Hamburg when seeking investment from COSCO in 2023. Cooperation at the EU-level is also beneficial to handle cases of economic coercion by foreign actors. For example, a foreign actor could threaten to reroute cargo flows from one European port to another.

Furthermore, the strategic framework takes a broad view by going beyond a narrow focus on ports or investments, looking at the **full maritime logistics hub function**. It does not just look at container terminals, but also at hinterland infrastructure, logistics support operations, and the regional impact of logistics operations. It would therefore contribute to protecting the EU maritime security interests outlined in the updated EU Maritime Security Strategy (EUMSS).[42]

Improving the existing toolbox

There are several areas in the current toolbox that could be improved with a strategic framework. First, at the time of writing, **FDI screening** varies widely between EU Member States, with some members such as Greece lacking screening altogether. An important step towards sharpening the toolbox is the proposed reform of the EU FDI Screening regulation, as announced by the European Commission in January 2024. Still, more than FDI screening is necessary to protect strategic autonomy, especially as the Member States all have different or unclear definitions of 'critical infrastructure', or different investment screening thresholds. Harmonising these differences would be beneficial.

Further, the **Anti-Coercion Instrument (ACI)** is mainly aimed at deterring economic coercion by third countries once the leverage of foreign influence is already present. The ACI focuses primarily on trade or investment restrictions. But coercion is also related to influencing the choice of logistics service providers or container carriers in favour of companies based in certain third countries. This limits the freedom of choice for logistics service providers and puts EU companies at a disadvantage. The strategic framework can amplify efforts against economic coercion by *managing* foreign involvement in the first place, taking away the leverage.

42 European Commission, "Joint Communication on the Update of the EU Maritime Security Strategy and Its Action Plan for an Enhanced EU Maritime Security", March 2023.

A strategic framework's broad view of seaports and related logistics can also ensure it provides added value beyond **CER and NIS2**. After all, CER only covers the aspects of seaports and logistics that are categorised as 'critical entities', while Member State definitions of critical infrastructure vary. NIS2 applies beyond the list of 'critical entities', and encompasses both 'essential entities' and 'important entities'. These are defined according to the entity's location, size, and sector.[43] Essential entities are subject to strict supervision, important entities are only subject to ex-post supervision. NIS2 focuses on the digital risks for network- and information systems, which the proposed strategic framework would help balance with economic considerations.

Current policy measures in the sector are mainly focused on hardware, but not on orgware or software, or the combination of the three. Though the revised Horizontal Cooperation Agreement pays attention to this issue, **vertical integration** in seaports and logistics is not yet sufficiently addressed. At present, only a few companies have significant market power as they dominate key stages throughout the supply chain, with negative effects on competition. **Unfair competition** also comes from Chinese companies' links to the state, which benefit them in the European market through state subsidies or other forms of preferential treatment. Meanwhile, European companies face many regulatory and non-regulatory barriers when in the Chinese market.

The impact of **port-innovation ecosystems** and the sensitive nature of third country presence in these systems is another point of attention lacking in current regulations. This especially holds with respect to PhD students from (military universities in) third countries, working on sensitive technologies in EU universities related to these port-innovation ecosystems. The screening of students is not part of the EU framework for FDI-investment screening (regulation 2019/452).

On the software side, existing instruments do not sufficiently cover **technology and digital infrastructure**. While the NIS2 Directive gives detailed consideration to cybersecurity risk-management measures – such as basic cyber hygiene practices, cybersecurity training, cloud computing services and AI – **port community systems (PCS)** are not specifically covered by the NIS 2 Directives. A PCS is a digital collaboration platform in seaports (and airports) that enables

43 European Commission, "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)", accessed August 2024.

the exchange of information between various public and private stakeholders related to the port call process, such as the port authority, customs, freight forwarders and shipping companies. PCS should be included in the broader NIS2 cybersecurity risk-management measures and reporting obligations. The crucial function of PCS for maritime import/export processes and the risks associated with PCSs from third countries – such as China's LOGINK – require specific attention in NIS2. This attention is in addition to the attention paid to vessel traffic services (VTS) in NIS2. Attention for PCS is especially needed given the large differences that currently exist between the port community systems of individual ports, while the EU does not yet have the authority to manage or coordinate a European port system. The strategic framework can provide a trajectory to harmonise port systems and bring all Member States to the same level.

NIS2 pays extensive attention to communication and information exchange and a joint approach to security incidents. It includes measures like the creation of computer security incident response teams (CSIRT) for each Member State that cooperate. In addition, NIS2 enables the exchange of relevant information in a network of national CSIRTs by developing and maintaining a European vulnerability database, through the establishment of a European cyber crisis liaison organisation network (EU-CyCLONe) or through cybersecurity information-sharing arrangements. The **strong development of AI** also demands specific attention, given the fast-growing applications of AI in maritime supply chains.

The EU's **AI Act** classifies different AI systems into three risk categories. Those with a 'minimal risk' will not be regulated. Systems with a 'limited risk' will have to submit to certain transparency obligations. The most burdensome regulation will apply to providers of systems that are classified as 'high risk', such as those used in critical infrastructures. High-risk are defined as AI systems intended to be used as safety components in the management and operations of critical digital infrastructures. These include maritime and port digital infrastructures (see Directive on the Resilience of Critical Entities (EU) 2022/2557), road traffic and the supply of water, gas, heating and electricity.[44]

44 European Commission, "Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)", article 55, June 2024.

This means that maritime transport and the functioning of ports are not seen as critical infrastructure from the AI Act perspective. A gap in the AI Act is related to practices that are based on data generated by third countries, but are related to logistics practices within the EU. These practices could potentially be used by third countries for manipulation or coercion. Below, AI applications are described that could be developed by and operated in China based on Chinese logistics and trade data. These extend to the European hinterland but are **immune to European AI legislation** that focuses on AI systems within the EU. However, 'critical infrastructure' as part of AI systems is classified as 'high risk' and AI-based manipulation techniques are prohibited, in addition to previous regulations that focus on the consequences of unfair trading practices that cause economic or financial harm to consumers.[45] The precise impact of AI on risks is still unknown and deserves further investigation and elaboration.

Finally, the creation of the European Ports Alliance, which is specifically focused on increasing cooperation against drug trafficking and organised crime, shows that there is an appetite for more coordination in the sector. A strategic framework can support the efforts to monitor foreign involvement and provide an information sharing mechanism at the EU level, with information contact points per Member State.

45 Ibid. article 29.

4 Conceptualising a strategic framework

Chapter 2 and 3 identified the need for a strategic framework. This chapter outlines the main functions of a strategic framework. It then conceptualises a draft design for a country-agnostic, EU-wide strategic policy framework for seaports and related logistics sector systems. It examines four segments of the maritime logistics hub function, and subsequently discusses hardware, orgware, and software for each level.

4.1 Main functions of the strategic policy framework

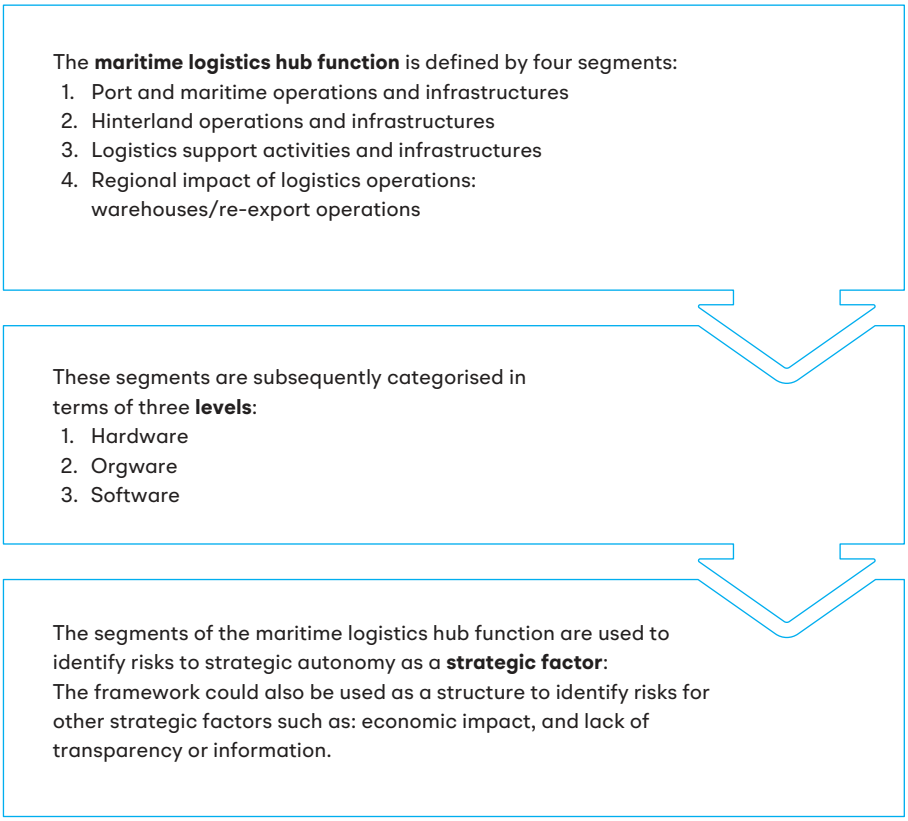
The strategic framework should have the following main functions:

- Allow the EU to optimise economic benefits from the role of third countries in the maritime-logistical sector while minimising negative side-effects to EU **strategic autonomy** and the social/environmental interests of the European public. The framework helps create an overview of relevant benefits and risks.
- Protect **market forces and economic interests** in the maritime-logistical sector where possible and prevent foreign state actors from dominating any part of the EU maritime-logistical sector.
- Provide a **coordinating mechanism** that prevents competition among EU Member States from undermining EU strategic autonomy.
- Outline how existing **policy instruments** are relevant and identify where policy instruments are still missing.
- Identify relevant **actors** and their roles and responsibilities.
- Be calibrated to, and serve as a lever for improving, the EU's **access** to the maritime-logistical sector of third countries.
- Be applicable **not exclusively** to China but also to any other non-EU actor as country-agnostic framework.
- Support **monitoring and information sharing** concerning foreign involvement in seaports and port-related logistics.
- Stimulate EU Member States to **identify strategic dependencies** in seaports and logistics, and to develop **contingency plans** in case intervention is needed.

4.2 Draft strategic framework

The following section presents a draft design for a country-agnostic EU-wide strategic policy framework for seaports and related logistics sector systems, outlined in Figure 1.

Figure 1 Outline of maritime logistics hub function and strategic framework



Seaports and related logistics sector systems

First, the concept of 'seaports and related logistics sector systems' will be unpacked, based on the previous study, '*Navigating an Uncertain Future*'.

The maritime logistics hub function focuses on activities related to transport, storage, and other logistics activities – including value-added logistics – and maritime services. These activities relate to goods with an overseas origin or

destination. It constitutes the entire complex of logistics functions surrounding the most important maritime logistics hubs in Europe: seaport hubs such as Antwerp, Hamburg, Rotterdam, Le Havre, Piraeus, Genoa, Valencia, Gdansk, Sines and other, involved in the global maritime transport function. The maritime logistics hub function focuses on four segments of **container activities** (figure 1), related to the impact of continued investments by Chinese companies, which is the main case study of this report.

The maritime logistics hub function is different from the **maritime manufacturing industry**, which concerns shipyards and maritime suppliers, hydraulic engineering and offshore contracting. An analysis of the dynamics in the entire maritime cluster shows that these two subsystems – port logistics and shipbuilding – have few mutual economic supply relationships and are largely independent, apart from the settlement pattern as there are a multitude of common maritime hotspots in the seaport environment.[46] In addition, the maritime logistics hub function must also be distinguished from the **industrial complexes** located in European seaports such as Marseille, Antwerp, Tarragona, or Rotterdam, which focus on oil refining and the chemical industry.

The maritime logistics hub function is divided into **four segments**:

1. *Port and maritime operations and infrastructures*: this includes (container) transshipment terminals in deep-sea ports (and related container activities such as empty depots), maritime shipping, characteristics of overseas trade and a third country's relationship with wider world trade. This segment is expressed in terms of investment in and ownership of port facilities – especially deep-sea container terminals in different ports and networks – ownership of container carriers, number of containers handled, the value and characteristics of cargo flows – strategic goods, weapons, etc. – or the magnitude and capacity of carriers controlled by third countries.

2. *Hinterland operations and infrastructures*: the development of hinterland infrastructures such as railroads, inland waterways, road infrastructure, shortsea shipping, pipelines, logistics/intermodal nodes and empty depots. This segment is expressed in terms of investment in and ownership of

46 B. Bart Kuipers, Michiel Nijdam, Onno de Jong & Walter Manshanden "Economische relaties zeevaartsector". Research for the Ministry of Infrastructure and Water Management. Rotterdam/ Delft: Erasmus RHV/TNO, March 2014.

intermodal hubs and terminals in the hinterland, ownership of intermodal or transportation companies operating in the hinterland, ownership of intermodal line infrastructure such as railroads/networks, numbers of hinterland containers handled, the value and characteristics of freight flows, and the capacity of intermodal carriers or other logistics companies linked to third countries.

3. *Logistics support activities and infrastructures*: maritime information technology and port community systems, logistics IT-platforms, chain management facilities, support activities such as insurance, finance, legal, etc. This segment concerns the use of IT-oriented activities in container terminal operations, such as the use of port community systems, software installed on logistics hardware in seaports and the use of AI in supply chain operations. It also involves office functions in legal, financial and other issues in maritime operations, located in various port cities.

4. *Regional impact of logistics operations*: investment in warehouse operations in the port region or in the (nearby) hinterland of seaports is often an important result of the development of deep-sea-container infrastructure in large hub-ports. The port of Piraeus, Greece, is a strong example. Investment by COSCO in container-terminal development resulted in derived investment in warehousing by firms such as HP, Huawei, ZTE and Samsung.[47] These warehouses are often devoted to re-export operations towards different EU-countries. This segment is reflected in the number, type and size of warehouse locations, and employment and added value effects, but also in related office developments by logistics service providers and trading offices.

47 Frans-Paul van der Putten, "Chinese Investment in the Port of Piraeus, Greece: The Relevance for the EU and the Netherlands", Clingendael Institute, 2014.

The four segments above define the maritime logistics hub function. These functions can subsequently be expressed at different levels. We define three levels according to which investments in the maritime logistics hub function can be categorised:[48]

1. *Hardware* refers to investment in and ownership of **'concrete' infrastructures** such as terminals, warehouses, computer hardware, transport equipment and other forms of physical infrastructures.
2. *Orgware* relates to the **organisational level**. Its main function is to enable the efficient and uninterrupted functioning of trade, logistical and transport processes. Orgware also needs to ensure a level playing field and reciprocity in competition with third countries, including fair logistical practices according to legal, transparency, environmental and labour standards. In addition, it deals with the way in which investments in particular infrastructures are orchestrated through broader policy or business concepts, such as vertical integration, or countries' global investment strategies such as China's Belt and Road Initiative. Other examples of orgware are port authority or corporate policies to cooperate or deal with threats, such as cyberattacks, through cyber hygiene policies. Orgware therefore has a close relationship with both hardware and software.
3. *Software* is used to optimise **logistics strategies** by maximising the effectiveness and utilisation of networks as well as avoiding bottlenecks. It generally functions in addition to hardware and orgware. Software is a crucial part of the maritime logistics hub function. It is needed for the execution of maritime trade, terminal operations, hinterland transport operations, logistics support functions and warehouse operations. Terminal automation, the loading of containers on ships, port community systems, vessel traffic services are all dependent on software. Currently, AI is a ubiquitous topic in the software domain.

The segments of the maritime logistics hub function and the three levels in which the maritime logistics hub function in countries in the EU are expressed, are used to **identify risks to the strategic autonomy** of the different elements of the maritime logistics hub function. The strategic framework identifies important parts of the hub function that are overlooked in most research but that may

48 Francesco Corman and Rudy Negenborn, "Accessibility of Ports and Networks", and Harry Geerlings, Bart Kuipers & Rob Zuiddijk "Ports and Networks: Strategies, Operations and Perspectives", 127-145, Abingdon: Routledge, 2018.

be crucial to the functioning and development of seaports. For example, it considers logistics support activities, including the port-innovation ecosystem of seaports. These are often devoted to strategic innovations for seaports such as AI, quantum computing and autonomous shipping. The detailed breakdown of the maritime-logistics hub function distinguishes this strategic framework from, for example, the framework used by Ghiretti et al. (2023).[49]

The next chapter will use the draft strategic framework outlined in Figure 2 to provide an overview of the negative side-effects of the impact of third countries on EU strategic autonomy (see Figure 3). It also gives an outline of existing relevant policy instruments, and identifies where policy instruments are missing (see Figure 4). The framework could also be used to determine the economic risks or potential for each segment, related to the impact of third countries. It could use economic indicators such as related trade flows, added value, and employment. For example, of the EU-China trade flows in 2023, approximately 55% was performed by sea transport and handled in EU ports.[50] The segments identified in the strategic framework can then be used in a **risk-benefit analysis** to balance risks to strategic autonomy with economic benefits.

49 Francesca Ghiretti, Meryem Gökten, Jacob Gunter, Olga Pindyuk, Gregor Sebastian, Plamen Tonchev & Zuzana Zavarská, "Research for TRAN Committee – Chinese Investments in European Maritime Infrastructure" (Brussels: European Parliament, Policy Department for Structural and Cohesion Policies, 2023), accessed August 2024.

50 Eurostat, "China-EU – International Trade in Goods Statistics", accessed August 2024.

Figure 2 Draft strategic framework: maritime logistics hub function

	Hardware	Software	Orgware
Port and maritime operations and infrastructures	– Investment in deep-sea terminals and additional port infra-structures – Ownership of land and port infrastructure – Computer hardware: IT-systems for terminal operations – Ships and other trans-port infrastructure and resulting cargo volumes	– Deep-sea terminal automation software – Port Community systems – Hinterland distribution software – AI-models/algorithms	– Efficient and uninter-rupted functioning of trade, logistical and transport processes – Level playing field and reciprocity in competition with third countries – Fair logistical prac-tices according to legal, transparency, environmental and labour standards
Hinterland operations and infrastructures	– Investment in hinter-land terminals – Investment in trans-port infrastructure – Ownership of land – Computer hardware: IT-systems for terminal operations – Ships and other trans-port infrastructure and resulting cargo volumes	– Inland terminal auto-mation software – Port Community systems – Hinterland distribution software – AI-models/algorithms	– Efficient and uninter-rupted functioning of trade, logistical and transport processes – Level playing field and reciprocity in competition with third countries – Fair logistical prac-tices according to legal, transparency, environmental and labour standards
Logistics support operations and infrastructures	– Office functions in seaports and large hinterland nodes for i.a. finance, legal, insurance, risk-development, strategy functions – Part of port-innovation ecosystem/knowledge infrastructure	– Port Community systems – AI-models/algorithms – Port innovation eco-systems – Financial transaction software	– Level playing field and reciprocity in competition with third countries – Fair practices according to legal, transparency, environmental and labour standards
Regional impact of logistical operations	– Warehouses in port and hinterland	– Warehouse software – AI-models/algorithms – Distribution software	– Level playing field and reciprocity in competition with third countries – Fair logistical prac-tices according to legal, transparency, environmental and labour standards

5 Potential risks of foreign involvement identified in the draft strategic framework

This chapter presents the draft strategic framework's breakdown of the maritime logistics hub function, with the aim to assess the risks to strategic autonomy. It discusses hardware, software, and orgware. Risk levels in the port and maritime infrastructures and the domain software are assessed as highest, including a serious risk to data disruption and therefore to strategic autonomy. Finally, this chapter illustrates how the EU instruments identified in Chapter 3 relate to strategic autonomy as identified in the framework.

Using the draft strategic framework in Figure 2, the risks to strategic autonomy can be assessed for every aspect of the maritime logistics hub function. This chapter will analyse the risks relating to hardware, software, and orgware in that order. This is summarised on the next page in Figure 3. The chapter then discusses the risks in relation to the EU instruments of Table 1.

5.1 Risk levels identified in the draft strategic framework: hardware

Port and maritime operations and infrastructures

When is a certain level of risk considered problematic for the strategic autonomy of the maritime logistics hub function? Concerning deep-sea terminal hardware and maritime operations, the most commonly used indicators are the **level of ownership**, **market share** and **trade volume** of a third country in the maritime hub function in the EU or in a given port: 'a higher market share also means higher dependency risks'[51], resulting in reduced autonomy. The question is, what are the risk levels that have a clear impact on the strategic autonomy of the maritime hub function?

51 Ghiretti, et al. (2023), 17.

Third countries have a strong impact on the strategic autonomy of a port if an entity related to the national authority of a third country gains a majority stake in the port authority or in the container terminal capacity of a given port. This is also the case if the trade flows handled by a port would be related to a third country for more than 50%. These cases could be problematic.

Piraeus is an example of a port where the Chinese SOE COSCO has a 67% stake in the Piraeus Port Authority, and has full ownership of the Piraeus Container Terminal. Equally important, most of the containerised cargo handled in the port is related to China. However, the share of Chinese containerised imports handled via the port of Piraeus into the EU is only 24%.[52] This is because of the large share of transhipment-containers handled in Piraeus, which are transported to other ports in the Mediterranean by feeder services.

52 Eurostat, "China-EU – International Trade in Goods Statistics", accessed August 2024.

Figure 3 Draft strategic framework: potential risks of foreign involvement to strategic autonomy of EU-ports and related logistics

	Hardware	Software	Orgware
Risk levels to strategic autonomy	No risk Limited risk: market share <10% Some risk: share 10-25% Serious risk: market share 25-50% Very serious risk: share >50%	No Risk Limited risk to data disruption Some risk to data disruption Serious risk to data disruption Very serious risk to data disruption	No risk Limited risk strategic autonomy Some risk to strategic autonomy Serious risk to strategic autonomy Very serious risk to strategic autonomy
Port & maritime operations and infrastructures	**Deep-sea terminals:** – High dependency on logistics, trade and investment strategies of third countries due to high market share – Dual use of terminals for commercial and military purposes **Ownership port infrastructure/ authority:** – Decision-making power shifting to third countries through high share of ownership **Computer hardware:** – Use of suppliers of third countries at the expense of local firms – Legacy systems **Cargo volumes:** – Vulnerability to trade sanctions and geo-political risks associated with conflicts with third countries. Potential negative effects on port employment/added value creation	**Deep-sea terminal systems:** – Legacy systems – Vulnerability to cyber-attacks – Third-country suppliers of IT-hard-ware and software – Vulnerability through modems or wireless transmitters of systems that are not connected to internet – Low data-hygiene personnel **Port Community systems:** – Concentration of data in one system – All information is processed, including sensitive/military data – Differences in security demands posed by port community systems in EU **AI-models/algorithms:** – Strategic sensitivity analyses, manipulation strategies and forecasts produced by third countries – Further research needed	**Efficient and uninterrupted functioning of trade:** – Lack of organisational measures in ports to increase cyber resilience – Low awareness and understanding of cyber threats **Level playing field and reciprocity:** – No level playing field or reciprocity by third countries (e.g. international relay) – Strong home market advantages by third countries – Preferential treatment of third countries when selecting sub-contractors – Low environmental awareness in the realisation of investment by third countries **Fair logistical practices:** – See above – Strong political pressure influencing business deals by SOEs of third countries – Coercion to use local service providers towards EU-service providers when exporting to third countries

Hinterland operations and infrastructures	**Hinterland terminals and intermodal networks:** – See above – Intermodal corridor development-strategies by third countries **Ownership port infra/ authorities:** – See above **Computer hardware:** – See above **Cargo volumes:** – Intermodal cargo volumes driven by seaport-volumes (see above)	**Inland terminal systems:** – Hinterland terminals increasingly connected to seaports via port community systems, systems of carriers, forwarders, etc. – Vulnerability of hinterland infrastructure because of legacy systems or lack of maintenance. – Data-hygiene SMEs on lower level **Port Community systems:** – See above **AI-models/algorithms:** – See above	**Efficient and uninterrupted functioning of trade:** – Lack of organisational measures in inland ports to increase cyber resilience – Low awareness and understanding cyber threats **Level playing field and reciprocity:** – See above **Fair logistical practices:** – See above
Logistics support operations and infrastructures	**Port-related office functions:** – Leak of sensitive information in assessing port business networks **Port-innovation ecosystem:** – Increased foreign influence or data leakage through participation of SOEs from third countries – Knowledge security risks in sensitive research areas through PhD-candidates or students of military universities from third countries	**Port-related office functions:** – Leak of sensitive information in assessing port business networks **Port-innovation ecosystem:** – Increased foreign influence or data leakage through participation of SOEs by third countries – Knowledge security risks in sensitive research areas through PhD-candidates or students of military universities from third countries	**Efficient and uninterrupted functioning of trade:** – Lack of organisational measures in logistics support operations to increase cyber resilience – Low awareness and understanding cyber threats **Level playing field and reciprocity:** – See above **Fair logistical practices:** – See above
Regional impact of logistical operations	**Warehouse districts:** – Trade disputes or geopolitical tensions with third countries impacting employment or added value creation	**Warehouse districts:** – Risks are limited through decentralised organisation and a large number of different organisations – There are some large e-commerce providers from China with operations (JD, Alibaba), but a minority share	**Efficient and uninterrupted functioning of trade:** – Lack of organisational measures in warehouse organisations or districts to increase cyber resilience – Low awareness and understanding cyber threats **Level playing field and reciprocity:** – See above **Fair logistical practices:** – See above

Source: expert interviews. Note: not an exhaustive enumeration but demonstrative of the functioning of the strategic framework.

A study for the European Parliament's Committee on Transport and Tourism (TRAN) carried out an initial risk assessment for the Port of Piraeus and identified **serious risks** for the local economic ecosystem of Piraeus and even for the national Greek economy, as well as cyber risks and potential leakage of sensitive data.[53] While a thorough risk assessment has not yet been carried out for the Port of Piraeus, it is clear that China's majority stakes and market share result in a high level of risk. In addition, a case study was conducted by the same authors for the **Port of Hamburg** on the investment by COSCO in Container Terminal Tollerort.[54] COSCO's shareholding in the Tollerort terminal was reduced from the originally intended 35% stake to 24.99%. It was concluded that this percentage did not result in significant direct power over strategy formation, nor in a no position in the supervisory board, making COSCO a 'silent partner' and thereby reducing the risks to strategic autonomy. A stake of more than 25% may therefore be considered **a significant threshold for such risks**. The volume of containerised trade passing though Hamburg related to China is around 30%.

Indicating the risk level to strategic autonomy is more complicated in a port like **Rotterdam**, where the ownership of the port authority is entirely Dutch. The market share of SOEs COSCO and CMG in the container-terminal capacity of the port of Rotterdam was only 8.2% in 2023. Including Hong Kong-based Hutchison Port Holdings would mean that the ownership share of Chinese container terminal operators would increase towards 73.3% in 2023 – however, Hutchison Port Holdings is not an SOE. The volume of deep-sea container cargo handled in the port of Rotterdam consists for more than 50% of flows originating from or sailing to China.[55] The containerised cargo related to China in the port of Rotterdam is largely for re-export and transit to the European hinterland of the port (77%), with the remaining 23% destined for the Dutch economy (23%), indicating the importance of the maritime logistics hub function for the Netherlands. This **high level of dependency on Chinese containerised trade** indicates a relatively significant level of risk for the strategic autonomy of the port of Rotterdam.

53 Ghiretti, et al. (2023), 21-27.

54 Ghiretti, et al. (2023), 28-33.

55 Frans-Paul van der Putten, Bart Kuipers & Xiaoxue Martin (2023) "China's strategic relevance to the port of Rotterdam". The Hague: Clingendael Institute, December 2023.

On a European scale, the share of Chinese SOE ownership in EU container terminals has been established at around 10%,[56] while Chinese deep-sea container flows accounted for a 16% share of total container volumes handled in the main European container ports in 2023 (total volumes include intra-European deep-sea and shortsea trade).[57] For individual ports, these shares could be significantly higher.

Based on the issues presented above, we propose that market and ownership shares of (SOEs of) third countries in the hardware domain of port and maritime operations and infrastructures **above 50%** can be considered as having a **very strong impact** on the level of strategic autonomy of a port. **Between 25-50%** this will be a **strong impact**, **between 10-25%** the impact is considered as '**to some extent**' and **below 10%** the impact is **limited** (see Figure 3). The combination of these three share proportions in one port, such as Piraeus, increases the impact on the level of strategic autonomy. For the EU ports, based on the ownership of container terminal capacity and trade volumes presented above, we assess the risks to strategic autonomy as 'to some extent'.

High market shares of third countries in container terminal facilities, port ownership and trade volumes may pose risks to the strategic autonomy of the maritime hub function. In the hardware domain, **a port may become dependent on logistics and transport strategies of third-country SOEs, driven by the interests and priorities of these third countries**. This may pose problems in times of geopolitical turbulence. In addition, ownership of the port or of port terminals can be problematic with regard to the dual use of the port for commercial and military purposes. Ownership of deep-sea-terminal infrastructure by a third-country SOE implies that terminal-hardware may be **made available to other SOEs from the same third country**. Fore example, Chinese port equipment suppliers like ZPMC or computer hardware suppliers like Huawei may be involved in terminals by COSCO or CMG, often at the expense of EU-suppliers. Ports handling high shares of cargo related to third countries are vulnerable to losing cargo because of geopolitically inspired measures by this third country. The fragmentation of the global economy due to geopolitical developments related to China would have serious and negative consequences for world trade and

56 Jacob Mardell, "COSCO Takes State in Hamburg Port Terminal". Mercator Institute for China Studies, September 2021.

57 Eurostat, "China-EU – International Trade in Goods Statistics", accessed August 2024.

would result in economic risks for port regions.[58] **Targeted trade restrictions by China** are well-known; examples are the Chinese export controls on gallium and germanium and on certain graphite products, and the informal import stop of Lithuanian products after Lithuania opened a Taiwanese Representative Office.

In addition to the hardware of container cranes, automated vehicles, other terminal infrastructure and the visiting sea vessels and other transport modes, a container terminal also has computer hardware. An important characteristic of this computer hardware is that these systems are often (very) outdated and also use outdated software. We will discuss the risks associated with these legacy systems in the software domain in the next section.

Hinterland operations and infrastructures

In contrast to the information available for seaports presented above, **information** on market shares, ownership structures and transport volume by (SOEs of) third countries related to hinterland terminal infrastructure and container flows is **not available** in a structured way. Therefore, it is complicated to produce an assessment of losses to strategic autonomy without further research. Most of the intermodal hinterland transport flows are fed from the maritime-logistics hubs by rail and inland waterway transport and have a large share of China related origins and destinations, as was mentioned above in relation to large transit and re-export flows. The availability of information relating to hinterland terminals is limited to case studies. These case studies have disappointing results in common. One example is the Budapest–Belgrade–Skopje–Athens/Piraeus railway corridor, which has been delayed, with volumes remaining low on an alternative connection between Piraeus and Budapest.[59]

Developments at Europe's largest inland port of Duisburg were a disappointment from the Chinese perspective. **Duisburg plays an important role in the network strategy of China and Chinese companies**.[60] The city of Duisburg presented itself

58 Shekhar Aiyar, Jiaqian Chen, Christian H Ebeke, Roberto Garcia-Saltos, Tryggvi Gudmundsson, Anna Ilyina, Alvar Kangur, Tansaya Kunaratskul, Sergio L. Rodriguez, Michele Ruta, Tatjana Schulze, Gabriel Soderberg, Juan P Trevino, "Geoeconomic Fragmentation and the Future of Multilateralism", International Monetary Fund, 2023.

59 Ghiretti, et al. (2023), 25.

60 Sinolytics, "China's International Logistics Ambitions with Four Key Impacts in Europe", accessed August 2024.

as the 'most Chinese city in Germany'[61] and is centrally located in intermodal networks with a strong presence of Chinese terminal operators COSCO and CMG in the north (port of Hamburg), in the west (ports of Rotterdam and Antwerp-Bruges), in the south (Italian ports) and in the east via the Silk Road, the rail link between China and Europe, which is part of the Belt and Road Initiative. Container throughput in Duisburg increased from 2.5 to 4.3 million TEU in 2011-2021. Duisburg is investing heavily in the development of its intermodal position in new terminal infrastructures, such as the Duisburg Gateway Terminal, and in warehouse capacity in the port. In addition, Chinese companies have made many investments in Duisburg and in the larger state of North Rhine-Westphalia. In Duisburg, investments increased from 3 to 60 companies in 2013-2020, of which 6 pertained to logistics services, such as the China Railway Container Transport Company (CRCT), related to the China State Railway Group. In North Rhine-Westphalia, investments increased to almost 1,100 companies, of which 25 were logistics service providers[62] Most of the newly established Chinese companies are small and focus on trade facilitation (wholesale and retail). Overall, these developments in the Port of Duisburg were considered risky from a competitive perspective by the Port of Rotterdam, especially regarding the aforementioned 1,100 new establishments by Chinese companies.

However, the mood in Duisburg has changed. The most prominent illustration was the exclusion of COSCO as a partner in the important Duisburg Gateway Terminal due to contractual issues with Duisburg Port and to the broader political discussion about the COSCO investment in the Tollerort Terminal in Hamburg.[63] Then, at the beginning of this year, Germany published a new port strategy with the central aim of sustainably strengthening the critical port infrastructure.[64] An important part of this is that investments and participations from third countries are not only examined on the basis of national security interests, or the interests of the respective federal state, but that it includes coordination from a European port perspective. The German ports must be able to trade

61 Michael Verfürden, "Duisburg will 'Deutschlands China-Stadt' sein—doch Jobs fehlen und die Zeit läuft ab", Handelsblatt, February 2021.

62 Bart Kuipers & Niels van Saase "Duisburg: New Mainport as Competitor for Mainport Rotterdam? Rotterdam", SmartPort, 2022.

63 Loveday Morris, Kate Brady, and Emily Rauhala, "Germany's 'China City' Doesn't Want You to Call It That Anymore" The Washington Post, May 2023.

64 German Federal Ministry for Digital and Transport [Bundesministerium für Digitales und Verkehr], "Die Nationale Hafenstrategie für die See- und Binnenhäfen", March 2024.

without critical dependencies. In this new strategy, the strong and one-sided focus on China previously displayed by Duisburg is out of question. Furthermore, investment in Duisburg remained below expectations.[65] In addition, the Silk Road rail connection has seen declining volumes, in the wake of Russia's invasion of Ukraine. As a result, container handling in the port of Duisburg fell by 10% in 2023 towards 3.6 million TEU, although the Houthi attacks in the Red Sea could now boost alternative Silk Road-routes.

In addition to these somewhat disappointing developments, rail infrastructure investments in Eastern European countries entail certain risks for strategic autonomy. The improvement of **intermodal connectivity from the South to the North** could theoretically result in the development of a rail axis connecting the **Baltic** with the Chinese-controlled **Mediterranean** ports. However, this still has a long way to go. Overall, we estimate market and ownership shares to be low, at less than 10%. China-related intermodal flows are certainly above 10% in major corridors to and from seaports, but probably below this percentage in the EU as a whole. A detailed assessment of these shares would have to be based on detailed knowledge of the European intermodal landscape, and requires further research.

Logistics support operations and infrastructures

Logistics support operations are needed to support trade and transport processes. They often consist of office functions in seaports and major hinterland hubs for a wide range of activities that enable physical port and maritime operations, such as insurance, finance, legal functions and head offices. This is an important part of the function of a **maritime logistics hub as a 'maritime city'**. Maritime logistics hub Singapore is the leading maritime city, the European hubs Rotterdam and Hamburg are in the top 10 of the ranking by Manon and DNV.[66] Port authorities are also part of this support function as the main facilitator of maritime processes through the harbour master; who is responsible for safety and security in the port and for a range of legal and IT functions, which are now integrated into port community systems in most ports. An important part of the logistics support operations and infrastructures is the **port innovation ecosystem**, including the knowledge infrastructure of specialised universities and research institutes. This innovation ecosystem supports both the competitive

65 Michael Verfürden, "Duisburg will 'Deutschlands China-Stadt' sein—doch Jobs fehlen und die Zeit läuft ab" Handelsblatt, February 2021.

66 Menon Economics & Det Norske Veritas, "The Leading Maritime Cities of the World 2024", 2024.

position of companies in the port and contributes to transitions, such as the transition to carbon-free maritime operations.

The hardware component is linked to the number of offices, employment, and added value of these activities and infrastructures. Statistics on these indicators are lacking as only a few individual ports make them available.[67] However, the importance of the maritime support function for strategic autonomy could be significant. Ghiretti et al. (2023) present two illustrations of the impact of China on this function. First, they indicate that **the entire port ecosystem in Pireaus is completely dependent on the Piraeus Port Authority, of which COSCO holds 67% of the shares**. The operation for this ecosystem is sensitive to disruptions. Second, they mention two COSCO offices in the city centre of Hamburg through which Chinese officials might be able to access networks, collect data, etc.

In the port of Rotterdam, there are examples of Chinese companies that are part of the port innovation ecosystem, and are part of research centres along with other innovative companies, which openly state that they are seeking knowledge regarding technological trends in the Rotterdam-based chemical industry.[68] In Duisburg, 13 of the 73 investments by companies with full or partial Chinese ownership are active in support functions, such as administrative and support services, professional, scientific and technical services, information and communication. Most of these companies have only 1 to 3 employees.[69] Chinese **PhD candidates** studying at technical universities – part of port innovation ecosystems – may also pose a risk if they come from **military universities and are active in sensitive technological research areas** such as AI and unmanned aircraft. Delft University of Technology has therefore stopped accepting Chinese PhD candidates from military universities or those who want to do a PhD in "sensitive research areas".[70]

The risks to strategic autonomy associated with these logistic support activities and infrastructures are considered **limited**, as Chinese involvement in logistic

67 Such as the port of Rotterdam, where about 28,000 jobs are related directly or indirectly to maritime business services, https://www.rotterdammaritimecapital.com/.

68 B. Kuipers & N. van Saase (2022), 43.

69 B. Kuipers & N. van Saase (2022), 31. This statistic is comparable to the situation in the Rotterdam region, based on public information on the Follow the Money website and Leiden Asia Centre.

70 Anabelle de Bruijn & Peer van Tetterode, "Ook Chinese Beurspromovendi in Nederland Rapporteren aan hun Ambassade".

support activities and infrastructures is also limited in most maritime logistics hubs, except for the port of Piraeus. The involvement of Chinese SOEs in port innovation ecosystems is limited to a few examples, but **information is lacking at the broader EU port level**. This points to the need for further research. Further, the risks to strategic autonomy associated with these logistic support activities and infrastructures need to be **balanced with economic benefits** due to the provision of support functions and the importance of sharing academic knowledge and disseminating innovations that benefit the port economy. This includes sharing this knowledge with Chinese academics with expertise in the field of sustainability (batteries, solar, EVs, etc.).

Regional impact of logistics operations

Most maritime logistics hubs in the EU have seen the emergence of warehouse districts full of warehouses that are heavily dependent on imports and re-exports from China. The port of Piraeus was mentioned earlier as an example. A very wide range of products manufactured in China are stored in these warehouses. However, among the logistics service providers specialising **in warehousing, Chinese companies play a subordinate role in most EU-countries**,[71] except for e-commerce companies such as JD (joint venture with COSCO) and Alibaba.

In terms of value, computers and related products are the most important import product originating from China. In terms of the number of containers, consumer goods for household and personal use are leading. The growth of re-exports, mainly of containerised products from China arriving in the Netherlands by sea to the EU hinterland, averaged 11.4% per year in 2007-2021.[72] This was reflected in the very strong growth of warehouse development, largely focused on Chinese seaborne import flows. For example, the footprint of warehouses in the Netherlands increased from 24 to 96 million square meters in 2000-2021, averaging 7.2% per year.[73]

71 As an illustration, in the Netherlands, only one Chinese-owned firm (KLG Europe, #28) was part of the top 100 logistics service providers, including large warehousing providers, https://vmn-logistiek.imgix.net/uploads/2023/06/top-100-logistiek-dienstverleners-2023-poster.pdf.

72 Frans-Paul van der Putten, Bart Kuipers & Xiaoxue Martin (2023) "China's strategic relevance to the port of Rotterdam". The Hague: Clingendael Institute, December 2023.

73 M. Merten Nefs, "Landscapes of Trade. Towards Sustainable Spatial Planning for the Logitistics Complex in the Netherlands", Delft: A+B | Architecture, 2024.

The **employment and added value generated** in the Netherlands in relation to container handling in the port of Rotterdam amounted to 83.4 thousand employees and 8.7 billion euros in added value in 2022, of which warehousing represents a very substantial part.[74] **China is responsible for more than half of the number of deep-sea containers handled in Rotterdam**. This means that trade tensions, boycotts or other measures by China with an impact on container volumes could have a strong economic impact on the logistical complex of the Dutch economy. This will also be the case in other EU countries with maritime logistical hub-ports, such as Belgium, Germany or Greece. However, the **risks of such an impact are limited**, as China is still highly dependent on its exports of manufactured products to the EU.

5.2 Risk levels identified in the draft strategic framework: software

Port and maritime operations and infrastructures

A deep-sea container terminal relies on terminal automation hardware and software, which connect terminal processes with shipping agents, container carriers, freight forwarders, hinterland transport companies, maritime service providers such as pilots, towing companies and boatmen, the port authorities, inspection services, customs authorities and more. Communication between these parties is usually performed using port community systems. However, terminal automation is also crucial to performing various terminal operations and the stowage process between the terminal and a container ship. Cyberattacks or system failures can bring container terminals to a standstill, such as the faulty Crowdstrike security update in July 2024. In short, **a high-risk software environment limits the degree of strategic autonomy, as it increases the likelihood of third-country influence on this domain**. In this section, we start by presenting risks to the strategic autonomy of terminal hardware and software due to some strong vulnerabilities. Next we focus on port community systems. Finally, AI is a strong potential risk to strategic autonomy. We describe the potential risks posed by AI applications of third countries.

74 Martijn Streng, Dominique van Keeken, Bart Kuipers & Larissa van der Lugt, "Economische Betekenis Containersector: Studie naar de Economische Betekenis van de Containeroverslag voor Nederland in de Rotterdamse Haven" (Rotterdam: Erasmus UPT, 2024).

The dependency on terminal hardware and software makes the matter of **legacy systems** – outdated hardware and software in use at container terminals – very urgent and a potential risk. These outdated systems often form the core of the terminal operating systems.[75] A central issue is how these legacy systems are integrated into the broader information ecosystems at terminals. They also need to be integrated into ever newer, more advanced data applications emerging around these legacy systems, such as cloud storage and AI applications. Replacing these systems is a very complex task and poses a risk to the continuity of operations.[76] This is an important point of attention mentioned in the literature[77] which was also confirmed in the interviews conducted for this research. Often, it is not even known exactly what a supplier installed twenty years ago. Such legacy systems are no longer updated in such cases, which may form an important security risk.

While many terminals in European ports find themselves in this situation, this is **a problem that receives little attention**. According to one of the interviewed experts involved in the implementation of terminal automation systems at the Port of Rotterdam, the systems of relatively modern terminals such as the Maasvlakte II terminals date from 2014 and can therefore now be classified as relatively old. And it is precisely this old hardware, operating with relatively outdated software, that is vulnerable to cyberattacks by third countries. To counter this, container terminals use advanced security measures using firewalls, practises such as network segmenting and/or network anomaly detection and regular updates. This vulnerability also applies to many ships that visit the terminals and that often have outdated systems as well. In addition, work routines at many container terminals can also be labelled as 'legacy' due to practices such as sharing security codes between terminal staff and suppliers. It is only since recently that new and more secure practices are being introduced in some ports, such as the 'secure chain' in the Port of Rotterdam.[78]

75 Quote by Jan Gardeitchik, senior lead digitalisation, Port of Rotterdam Authority, cited in: E. Savelsberg et al., "Upgrading Legacy Systems in Ports and Terminals: A 'How-to-Guide,'" *Port Technology*, 4-6. edition 99, August 2020

76 Ibid.

77 For example, in: Leonard Heilig and Stefan Voß, "Information Systems in Seaports: A Categorization and Overview" *Information Technology and Management* 18, no. 3 (September 2017): 179-201.

78 Portbase, "Secure Chain Program", accessed August 2024.

There is a distinction between **terminal hardware that is connected to the internet and hardware that is disconnected from the internet**. Container cranes are usually disconnected from the internet and are controlled by separate hardware and software that allows the cranes to perform relatively simple tasks. However, by adding a modem, the cranes can be connected to the internet and can then be influenced remotely and, for example, stopped. This is the core of the recent controversy about the Chinese ZPMC cranes. Also, the interviewed experts state that certain container terminal systems can be influenced from outside the terminal using wireless transmitters that can easily take over control, making these systems vulnerable.

The '**terminal operating system**' controls the terminal as a whole and is connected to external sources via the internet and the port community system. From the perspective of critical infrastructure, the terminal operating system is the most critical element of container terminals. The terminal operating system is protected by firewalls against external threats. Such systems are secure in principle, but there is no guarantee that they are completely impenetrable. It is possible to monitor and view data, influence terminal processes or shut down the terminal if the terminal operating system is penetrated. When such a penetration occurs, **it becomes possible to identify military cargo based on the IMO cargo code**. Such military cargo is often assigned a separate place at a terminal, which becomes visible in this way. It is illustrative of the importance of information on cargo flows that detailed data on Chinese export flows are manipulated by China and are therefore not very reliable. In China, this information is often even considered a state secret.[79] However, cargo information is often available in other ways than via the complicated route of a terminal operating system. Governments and companies in the EU are regularly hacked by parties from within third countries, which could in principle also happen at customs or anywhere else in the port ecosystem.

Several of the interviewed experts emphasise that instead of laboriously shutting down container cranes or terminals, **shutting down an entire port, for example by disrupting the power supply or blocking the port by sinking a ship in a strategic location, forms a much greater threat**. The recent Crowdstrike incident showed that there are global implications when a disruption occurs in

79 See: The Economist, "Is China Understating Its Own Export Success?" December 2023, and The Economist, "Why Is Xi Jinping Building Secret Commodity Stockpiles?" July 2024.

connected networks, or when there are issues with providers that have access to the core of networks, such as security companies, when updating the terminal operating system of container terminals. Several responses to the Crowdstrike incident therefore warned against giving external service providers access to the core of the computer network,[80] such as the terminal operating system of a container terminal. However, electronic equipment from Chinese companies such as Huawei – and to a lesser extent scanning equipment from Nuctech – is used by private enterprises and authorities in most EU ports. In addition, China is a major supplier in the 'global value chain' of many electronic systems. **Electronic components produced in China are used in almost all electronic systems in the port and control systems are used with 'backdoors'** in hardware and software that make it possible to influence operations, according to experts interviewed.

Port community systems are also susceptible to risks. Firstly, due to the concentration of digital information in one system, since the greater this concentration, the greater the vulnerability to attacks by third countries. The Crowdstrike and Zyxel incidents showed that even well-secured companies are in principle vulnerable.[81] These incidents have prompted warnings against **relying on just one or a few critical computer systems**, for instance on just one supplier for critical digital information for port processes via the port community system.

A second reason to be cautious regarding such concentration pertains to the characteristics of information, as all information about goods flows is included in the port community system based on consignment notes. Third, the Chinese **LOGINK**, also known as the National Public Information Platform for Transportation and Logistics, is a port community system that collects international logistics data flows in one platform and is used for smart port ecosystems, among other things.[82] The government-linked company was founded in 2011 by the Chinese Ministry of Transport and fits into China's **Digital Silk Road,**

80 Josephine Wolff, "Software Crash Exposes Tension Between Security and Competition", Financial Times, July 2024.

81 Hackers were able to gain access to 22 Danish energy companies almost simultaneously through a critical vulnerability in Zyxel firewalls, which are devices designed to keep malicious traffic out of the company network. These companies had either neglected to install firewall security updates under the (incorrect) assumption that their IT provider would install the updates, or they simply did not know that a Zyxel device was on the network. Source: ABN AMRO, "Cyberaanval Schudt Ondernemer Lang Niet Altijd Wakker", accessed August 2024.

82 Frans-Paul van der Putten, Xiaoxue Martin & Bart Kuipers (2022), "Navigating an Uncertain Future", Clingendael Report, 92.

which clashes with the European open vision of digital connectivity. LOGINK is presented by the Chinese government as the technical standard for information exchange in logistics. LOGINK now works with partners all over the world. LOGINK is a member of the IPCSA, the organisation of port community systems, and cooperates internationally in this organisation.

Fourth, there are **major differences in the security of port community systems in EU-ports**, while most port community systems are interconnected. The vulnerability of port community systems is currently **underexposed**. The European cyber resilience directive NIS2 does not mention port community systems. There are networks of terminals where information from poorly secured ports can be passed on to well-secured ports and vice versa. **This necessitates a pan-European approach. Establishing such an approach is however complex** because the applied security requirements for port community systems differ significantly between ports in North-Western Europe and the Mediterranean, according to one of the experts interviewed.

The advent of AI is another potential source of risk. AI systems focus on collecting large amounts of data that are analysed in algorithm-based models, aimed at training self-learning, generative applications. The maritime sector is an example of a sector that generates a lot of operational and trade data. **This is especially true for Chinese data, based on China's extensive role in global trade.** Through pattern recognition, weaknesses in maritime goods flows can be analysed based on this data, both at sea and inland. For example, what were the consequences of the blockade of the Suez Canal or the Red Sea by Houthi rebels for European goods flows? AI can be used to visualise which critical goods flows a country depends on, and **to produce knowledge about the effects of disruptions based on the patterns of these flows**. Based on demand forecasting, goods flows can be disrupted by gaining insight into bottlenecks. For example: when is the demand for which goods highest? That is when disruptions would have the greatest impact. Models can be trained to exploit weaknesses in trading systems; for example by predicting the negative effects of attacks by Houthis on the German food market. With such models, third countries can learn which disruptions have the greatest consequences, such as two consecutive incidents in the Suez Canal. By subtly executing these disruptions, smaller disruptions can also occur in the global trading system.

According to the interviewed AI expert, such AI applications are now likely to be developed by third countries which could pose risks to strategic autonomy,

especially in increasingly connected trade chains. The AI applications described above could be **developed by and operated in China based on Chinese logistics and trade data**, which may extend to the European hinterland but **do not fall under European AI legislation**, which focuses on AI systems within the EU. However, 'critical infrastructure' as part of AI systems is classified as 'high risk'.[83] AI-based manipulation techniques are prohibited. There are also older regulations that focus on the consequences of unfair trading practices that lead to economic or financial harm to consumers. The precise impact of AI on risks is still unknown and calls for further investigation and elaboration.

In addition, the strong rise of **cloud services is a risk to strategic autonomy**. The cloud is increasingly seen as a critical infrastructure. Ideally, these cloud services should take place within the systems of European providers, as this would strengthen European strategic autonomy. This certainly applies to military applications in the maritime logistics domain. Research by Dutch government services identified a large number of risks surrounding cloud services, of which the lack of clarity about where the data centres are physically located is just one. At present, there is an oligopoly of three American and one Chinese cloud capacity provider.[84]

Based on the above **we assess the risks to disruptions in the software-domain as high**. This report thus concurs fully with the conclusion by Ghiretti et al. (2023, p. 9) that: "**Data and analysis of Chinese presence in cyber/data management in ports is poor and so is the analysis of related risks.** Further research to collect data on the risks of Chinese companies' involvement in cyber and data security in critical infrastructures would provide a strong basis to inform Member States and develop related policies."

Hinterland operations and infrastructures

A well-functioning network of intermodal terminals from seaports to the hinterland (and vice versa) is of great importance for sustainable transport in the EU. Without inland shipping, rail and short sea operations, road networks would be completely overloaded. The road transport system would also not

83 European Commission, "Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)", (9.), June 2024

84 The Economist, "Do the Costs of the Cloud Outweigh the Benefits?", July 2021

be able to handle this additional volume for the simple lack of truck drivers and infrastructure capacity. Furthermore, **inland transport hubs are highly vulnerable to cyberattacks on critical maritime objects** such as locks or bridges or on the complex railway planning systems. The issue of legacy systems is also relevant for hinterland infrastructure in the EU. There are general maintenance backlogs of these infrastructures in a number of EU countries, making them vulnerable to cyberattacks from third countries.

Inland terminals are increasingly connected to deep-sea terminal operations via port community systems or via the systems of carriers or forwarders. This means that **most digital risks related to deep-sea terminals are the same for hinterland terminals**. Vulnerabilities in data hygiene and cyber prevention may be a bigger problem for SMEs operating inland terminals,[85] although there are examples of digital frontrunners in the intermodal hinterland network. Hinterland terminals in the EU also call for further investigation. To conclude: **we also assess risks to hinterland operations and networks in the software domain as high**.

Logistics support operations and infrastructures

The risks to strategic autonomy associated with logistic support activities and infrastructures in the software domain are considered **limited, mainly because of the very small number of Chinese companies in this field** in important port cities such as Duisburg or Rotterdam. However, there are some points of attention in the hardware domain, such as the presence of offices related to SOEs in port cities that could access networks, collect data, etc. There are also examples of companies from third countries that are part of the port innovation ecosystem, and openly seek knowledge regarding technological trends. These trends and innovation agendas certainly may relate to fields such as AI or quantum computing, which are strong priorities in Chinese scientific research.[86] We also referred to the sensitive issue of Chinese PhD candidates studying at technical universities, who may also pose a risk if they come from military universities and are active in sensitive technological research areas, such as **quantum computing and AI**.

85 See: ABN AMRO (2024).

86 The Economist, "China Has Become a Scientific Superpower", June 2024.

Regional impact of logistics operations

Software used in warehouses enables efficient warehouse operations and connects these warehouses with distribution systems towards the customer, often organised via e-commerce processes. As stated above, besides a small number of large e-commerce giants like Alibaba and JD, most of the logistics service providers in warehouse districts in the EU are companies based in the EU or the US, such as DHL, CEVA, DSV, GXO, Amazon or Kuehne+Nagel. Data of customers based in the EU are an important issue and the abuse of personal data by companies in third countries is a risk, but this goes beyond the maritime logistics hub function. There is always a risk to strategic autonomy of cyberattacks on the networks of these logistics service providers and warehouse companies, but given the **distributed and decentralised patterns of warehouses**, we rate this risk as **very limited to non-existing**.

5.3 Risk levels identified in the draft strategic framework: orgware

Port and maritime operations and infrastructures

Orgware concerns organisational agreements in container operations and the import, export and transit of goods in ports. Limiting risks around data and cyber resilience is mainly achieved by organisational measures. In many ports, government and industry collaborate to increase cyber resilience and, in the EU, NIS2 focuses on this. The participation of third-country related SOEs in such collaboration initiatives poses a risk. Certain risks are therefore discussed without the presence of, for example, China-related terminal operators such as COSCO and CMP.

The **larger goal** of organisational and policy agreements in orgware is:

a. to ensure the **efficient and uninterrupted** functioning of trade, logistical and transport processes via EU ports,
b. to create a **level playing field** and **reciprocity** in competition with third countries,
c. to realise **fair logistical practices** according to legal, transparency, environmental and labour standards.

Orgware is an important connection between hardware and software. **Software problems can be solved by using orgware and especially by increasing awareness of the need for cyber resilience.** It is mainly through organisational measures that risks can be reduced, such as regular software

updates, maintaining high-quality data hygiene, and through innovations such as the introduction of organisational policies like the '**secure chains**'. This secure chain is a closed logistics chain through which authorised parties digitally grant each other the right to pick up a container at container terminals. Only a carrier authorised via the chain of trust can report its arrival at the terminal in advance and then show up there. Sharing PIN codes with each other is now a thing of the past. Organisational measures also relate to, for example, the screening of employees who work at container terminals.

Under orgware we can also classify the practices of the Chinese government to gain influence on different parties in the chain through the highly intertwined **horizontal and also vertical cooperation**. Ghiretti et al. (2023:19) imply that **competing with COSCO is competing with the Chinese state** through the SASAC vehicle.[87] They also point to the lack of reciprocity, since COSCO enjoys extensive protection through extremely restrictive cabotage laws in China resulting in a protective home market advantage. Non-Chinese shippers are excluded from international relay and domestic/domestic shipping in China, In the EU, a foreign company like COSCO can operate all types of shipping, especially if it invests in a local subsidiary.[88] This means that there is no level playing field and reciprocity, which poses a risk for strategic autonomy.

Within container shipping, there is a strong drive towards horizontal integration by most carriers, including COSCO. COSCO works in the Ocean Alliance together with CMA CGM and Evergreen. This means that a lot of **operational data is shared**, also between the terminal organisations that are related to these shipping companies. **The characteristic of 'intertwining' in the container sector is therefore a structural risk.**

Several carriers have changed their strategy from horizontal to vertical integration to become an 'integrator of the seas'. Maersk is leading this strategic move and others have followed, notably CMA CGM, while COSCO's efforts have been limited. These vertically integrated carriers have invested in Europe-wide

87 State-owned Assets Supervision and Administration Commission of the State Council.

88 Jacob Gunter, "Levelling the playing field in maritime shipping", Mercator Institute for Chinese Studies, August 2021; Francesca Ghiretti, Jacob Gunter, Gregor Sebastian, Meryem Gökten, Olga Pindyuk, Zuzana Zavarská, Plamen Tonchev, "Chinese Investments in European Maritime Infrastructure", European Parliament, Policy Department for Structural and Cohesion Policies, September 2023.

feeder services and intermodal operators,[89] and in logistics activities far removed from the core container business, such as air freight operations and publishing. COSCO has shown limited vertical integration activities in the logistics chain. It invested in a railway company connecting Piraeus to the Silk Road in 2019[90] and set up a joint venture with JD in 2019, after Alibaba and Amazon became the world's third largest e-commerce retailer. It also acquired Italian supply chain services provider Trasgo in January 2024 through a joint venture with Fratelli Cosulich, a diversified company from Italy that, in addition to its steel business, offers various shipping and supply chain services. **COSCO is therefore slowly implementing its vertical integration strategy in the EU.**

Moreover, with respect to fair logistical practices there are many points of attention with respect to **legal, transparency, environmental and labour standards**. Ghiretti et al. (2023: 23) give some examples concerning the port of Piraeus such as the advantage for COSCO of Chinese state's political support to ensure better contractual terms, the absence of an environmental impact assessment, using Chinese subcontractors instead of Greek for the construction of the container terminal, concerns about pollution caused in the port, and in general a low environmental awareness and strikes resulting from serious labour disputes, causing declining throughput volumes of the port. Issues related to unfair logistics practices are also found in other ports. **Freight forwarders exporting cargo from the EU into China are forced to make use of COSCO and other Chinese logistics service providers.** If they do not, containers could be delayed or the container must undergo additional inspections in the Chinese port of entry.[91] This is a form of coercion, aimed at influencing the choice of shippers and logistics service providers towards Chinese parties.

Hinterland operations and infrastructures, logistics support and regional operations

There is a **lack of information** on the orgware domain in the hinterland, in the urban area where most firms are located in logistics support functions and the port-innovation ecosystem, and in the warehouse districts.

89 Hubert Paridaens & Theo Notteboom, "Logistics integration strategies in container shipping: A multiple case-study on Maersk Line, MSC and CMA CGM", Research in Transportation Business & Management 45 (2022), December 2022.

90 Ghiretti, et al. (2023), 22.

91 Frans-Paul van der Putten, Bart Kuipers & Xiaoxue Martin (2023) "China's strategic relevance to the port of Rotterdam". The Hague: Clingendael Institute, December 2023.

Elaboration

The draft strategic framework presented a **detailed breakdown** of the maritime logistics hub function and serves to assess risks to strategic autonomy of the different parts of the maritime logistics hub function. It made clear that **risk levels in the port and maritime infrastructures and the software domain are assessed as highest**. With respect to port and maritime operations and software, the software domain is even assessed as posing a serious risk to strategic autonomy through data disruption, because of the potential for third countries to influence this function.

Further research into some elements about which **information is lacking**, such as:

- threats to strategic autonomy in hinterland networks and terminals; most research has been performed on seaports
- the involvement of third countries in port-innovation ecosystems
- AI developments in deep-sea ports and maritime networks
- software developments and data applications in hinterland networks
- an economic approach to risk; what are employment and added value consequences for the four functions in maritime logistics hubs?

The risks associated with strategic autonomy are highest in ports and maritime operations and infrastructures, but this is also the part of maritime logistics infrastructures that has been researched most extensively.

5.4 EU Instruments aimed at limiting risks to strategic autonomy relating to the European seaports and logistics

Finally, we apply the EU-instruments listed in Chapter 3 to the risks relating to strategic autonomy as identified in the framework (see Figure 4). This is not a detailed and critical assessment of the strong and weak points of different EU-instruments, but a **broad assessment of the suitability of the instruments for use within the framework for strategic autonomy**. These instruments require a process of regular updating because of the strong effects of new technology on ports, such as in the area of artificial intelligence.

The identified risk-levels are highest in the ‘software’ domain. This means that instruments should limit ‘software-related’ risks. That means attention for instruments applied for:

- **Data security**. According to the interviewed experts, data information is potentially visible down to the smallest details. Logistics data is critical for strategic autonomy, especially data on military good flows (visible via IM-code), data on sensitive cargo such as rare-earth elements, hi-tech goods, and strategic goods with potential dual-use applications.
- **Data manipulation**. Data manipulation is common practice in trade and there are lots of opportunities for malicious third countries. Also, AI is having a rapidly growing impact. There is a large amount of data available from carriers, forwarders, port community systems, customs, etc. in large logistics nodes such as seaports and large inland ports.
- **Safety risks for container terminals**. Terminal-automation systems are assessed as being vulnerable, especially when these systems are connected to the internet. In individual terminal hardware such as container cranes, most of the software is isolated and of an operational character, which reduces vulnerability. But terminal-automation systems are connected to the internet and to other terminals in European terminal networks, which means that data security of container terminals has a European-wide impact. Safety risks for container terminals are also related to outdated IT-systems and software ("legacy systems") with no or very limited maintenance/updates and with possibilities to manipulate terminal processes from outside. In addition, a risk is that working practices by terminal personnel are not at the required or desired level.

Figure 4 Draft strategic framework: relevant existing EU-instruments and necessary additional instruments

	Hardware	Software	Orgware
Port & maritime operations and infrastructures	– Investment in deep-sea terminals and additional port infrastructures – Ownership of land and port infrastructure *Revised EU FDI Regulation & Anti Coercion Instrument* – Computer hardware: IT-systems for terminal operations *NIS2* – Ships and other transport infrastructure and resulting cargo volumes *No instruments available*	– Deep-sea terminal automation software *NIS2 & CER* – Port Community systems *No specific instruments available* – Hinterland distribution software *NIS2 & CER* – AI-models/algorithms *AI Act: continuing instrument development needed*	– Efficient and uninterrupted functioning of trade, logistical and transport processes – Level playing field and reciprocity in competition with third countries – Fair logistical practices according to legal, transparency, environmental and labour standards *Anti-Coercion Instrument* *Horizontal co-operation agreement*
Hinterland operations and infrastructures	– Investment in hinterland terminals – Investment in transport infrastructure – Ownership of land – Computer hardware: IT-systems for terminal operations – Ships and other transport infrastructure and resulting cargo volumes *See above*	– Inland terminal automation software – Port Community systems – Hinterland distribution software – AI-models/algorithms *See above*	– Efficient and uninterrupted functioning of trade, logistical and transport processes – Level playing field and reciprocity in competition with third countries – Fair logistical practices according to legal, transparency, environmental and labour standards *See above*
Logistics support operations and infrastructures	– Office functions in seaports and large hinterland nodes for i.a. finance, legal, insurance, risk-development, strategy functions – Part of port-innovation ecosystem/knowledge infrastructure *NIS2 and CER*	– Port Community systems – AI-models/algorithms – Port innovation ecosystems – Financial transaction software *NIS2 and CER +* *See above*	– Level playing field and reciprocity in competition with third countries – Fair practices according to legal, transparency, environmental and labour standards *See above*
Regional impact of logistical operations	– Warehouses in port and hinterland *No instruments available*	– Warehouse software – AI-models/algorithms – Distribution software *See above*	– Level playing field and reciprocity in competition with third countries – Fair logistical practices according to legal, transparency, environmental and labour standards *See above*

First, foreign direct investments by third countries in the **different hardware categories** could threaten strategic autonomy when thresholds are exceeded in certain ports, port ranges or in the European seaport infrastructure as a whole. As stated above, China controls roughly 10% of container terminal throughput in the EU. For individual ports and terminals this percentage may be higher. Chinese container carrier COSCO has a 67% stake in the Piraeus Port Authority and full ownership of Piraeus Container Terminal.

Instruments related to investments in the different hardware categories are covered in the revised EU framework for foreign direct investment screening, the **Revised EU FDI Regulation** (see Table 1).[92] This framework covers investments of any kind by a foreign investor (Article 2). The broad and general nature of this investment screening instrument fits well with the four elements identified in the hardware segment in the maritime logistics hub function. Article 4 concerns the determination of whether a foreign direct investment is likely to affect security or public order, taking into account the potential effects on critical infrastructure and on land and real estate essential to the use of such infrastructure. Article 4 links foreign direct investors to third country governments. The thresholds regarding third country ownership may vary for each individual port in terms of size, function, location, governance, use and other characteristics to be considered in the screening process.

It is important to not only adopt **quantitative** but also **qualitative** screening methods, given the different effects of investments for each port. The use of seaports for military purposes is a very important criterion regarding the screening of foreign direct investment by third countries. In addition, **the Anti-Coercion Instrument** addresses investments by third countries.[93] This concerns the influence of investments on either preventing or securing the the withdrawal, modification or approval of a certain act, thus interfering with the legitimate sovereign choice of the Union or a Member State.

Safety measures at all seaports in EU-countries must meet basic minimum requirements. This relates to port community systems and container terminals. This means attention for outdated IT-systems and regular updates and system

92 European Commission, "Regulation (EU) 2019/452 Establishing a Framework for the Screening of Foreign Direct Investments into the Union", March 2019.

93 The European Parliament and the Council of the European Union, "On the Protection of the Union and its Member States from Economic Coercion by Third Countries", November 2023.

maintenance. The issue of **legacy systems** in the **computer hardware domain** is treated in NIS2 (Article 49) where cyber hygiene policies are mentioned comprising a common baseline set of practices, including software and hardware updates, password changes, the management of new installs et cetera.

There are **no known instruments yet** regarding the regulation of maximum levels of trade and **container flows from third countries** in different ports. The objective of most seaports is still to increase the levels of container handling, with a view to the economic impact of cargo handling (direct and indirect). The concept of strategic autonomy has an indirect effect on the growth of cargo flows if it results in concepts such as near-sourcing, reshoring and regionalisation of global value chains.

There are no specific instruments available on risks related to the **logistic support function**, but the general instruments CER and NIS2 cover the issues related to these functions. More information is needed on the typical threats to strategic autonomy relating to the logistic support function.

Regarding investments in warehouses as a key outcome of the regional impact of the maritime logistics hub function, no critical thresholds have been defined regarding maximum levels of storage of goods from third countries. As with container flows, most EU countries are trying to increase the number of warehouses with a view to regional-economic goals such as job creation and added value generation.

Developments in the field of **software** applications in the maritime industry are dynamic due to the rise of **Artificial Intelligence**. AI can provide real-time visibility into the supply chain from origin to destination and from feedstock to finished product.[94] This can result in risks to strategic autonomy related to the availability of trade and logistics data to third countries with possibilities of manipulation. It is widely recognised that AI can disrupt business models. The impact of AI-powered algorithms is not clear as these algorithms are currently being designed, but above we explained possible practices by third countries that may disrupt maritime supply chain operations. It is believed that building powerful AI applications will optimise the competitive position of maritime companies.

94 Dirk Koppenol & Hannah Mosmans, "Dream Big, Start Small: AI in Transport and Logistics. Opportunities for Business, Government, and Science", (Rotterdam: SmartPort/Erasmus UPT, 2023).

Investing in AI is currently a priority in logistics and business applications in China,[95] where the government is promoting data sharing. The datafication of the industry is a strong driver contributing to economic growth. The AI Act entered into force in August 2024 and will be fully applicable after two years, with some exceptions. A key focus area is third countries' AI practices based on EU trade and logistics data.

The software level of the maritime logistics hub function is vulnerable to **cyberattacks**, **espionage** of trade information – for instance relating to trade in sensitive products or military equipment – and **sabotage** and other disruptions caused by third countries. The NIS2 and CER directives are aimed at these vulnerabilities. In addition, **Port Community Systems** also require special attention in the update of EU-instruments due to the central role of PCS-infrastructure in major seaports, which increases vulnerability.

Orgware is related to various business processes, organisational concepts or geostrategic concepts initiated by third countries. Orgware can pose a risk to strategic autonomy when ports and hinterland infrastructure become part of larger organisational strategies of third countries. China's **Belt and Road Initiative** is an example of such a strategic, geopolitical entity in which seaports can become part of larger frameworks, with port networks being managed according to the larger strategic goals set out in the Belt and Road priorities.

Vertical integration of the different elements within larger maritime supply chains is a practice that in some cases is directly linked to the impact of companies supported by governments in third countries.[96] There is a risk that individual elements serve larger purposes related to strategic goals and that vertically integrated firms can exchange information in an upstream market, gain market power, and collude to raise the price of a key input for a downstream market.[97] **Coercion** is relevant in several aspects of the maritime hub function, such as the non-reciprocal nature of investments or the provision of logistics services – such as cabotage or international relay – by third countries.

95 The Economist, "China Is Shoring Up the Great Firewall for the AI Age", December 2023.

96 European Commission, "Evaluation of Commission Regulation (EC) N° 906/2009 of 28 September 2009 on the application of Article 81(3) of the Treaty to certain categories of agreements, decisions and concerted practices between liner shipping companies (consortia)", 2023.

97 European Commission, "Guidelines on the Applicability of Article 101 of the Treaty on the Functioning of the European Union to Horizontal Co-operation Agreements", 2023.

It can also take the form of strongly influencing the choice of logistics service providers in favour of providers from certain third countries when exporting to these countries. EU instruments that focus on orgware are available. The **Anti-Coercion instrument** is a broad and flexible regulation aimed at measures taken by third countries. The Belt and Road Initiative mainly involves investments in diverse infrastructures and is therefore linked to the **Revised EU FDI Regulation**. Vertical integration is addressed in the recent update of the Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to **horizontal co-operation agreement** (see Table 1).[98]

Figure 4 presents the instruments available at EU level to counter the risks related to foreign involvement. We find that most instruments provide the necessary measures. However, as discussed in Chapter 3, the toolbox is not implemented equally by the European Member States. The combined instruments for screening foreign direct investments and the anti-coercion instrument are complementary. However, the ACI entered into force on 27 December 2023, and the revised EU FDI Regulation was published on 24 January 2024. It takes time to implement these instruments in all EU countries. This also applies to the CER directive and NIS2. Figure 4 does not provide information on the actual implementation of these instruments in different EU countries.

98 ibid.

6 Steps towards developing and implementing a strategic framework

This chapter discusses the next steps towards developing and implementing the framework conceptualised in the previous chapters. It also lists the division of responsibilities between EU institutions, Member States, and the sector stakeholders, and potential obstacles and windows of opportunity for the realisation of the strategic framework. Finally, this chapter offers suggestions for the narrative around the strategic framework.

6.1 Steps

The strategic framework presented in the previous chapters is a draft, which needs to be developed further in collaboration with the EU and its Member States. The Dutch government has already begun exploring possibilities towards introducing such a strategic framework, meeting with the EU's DG Move and several other Member State stakeholders to gather information on their positions and input towards a framework. **This process needs to be continued to further develop and gain support for a strategic framework.** The discussions so far indicate that these efforts are most likely to succeed if the Dutch government first focuses on obtaining the support of several other Member States, before jointly lobbying at the EU-level for legislation. This means that the risks related to foreign involvement in the maritime logistics hub function should continue to be discussed with other Member States, and the framework should be sufficiently flexible to incorporate their concerns and input.

The Member States that have not yet been consulted should be **categorised** according to the three groups outlined in Chapter 2:

a. Countries that regard foreign involvement as a potential security threat that is urgent and requires coordination with other EU Member States or with the EU as a whole.
b. Countries that regard foreign involvement as a potential security threat, but seem to prefer to address this at the national level.

c. Countries that do not view foreign involvement in seaports and related logistics as a major security issue, or as the most important issue.

The effort to build support for a framework should first be on countries belonging to category (a). Countries in category (b) can only be convinced of the need for a strategic framework if there is enough support among other Member States to embark on a joint approach. To get the support of countries in category (c), the framework will have to be able to address not only security risks or risks to strategic autonomy, but also economic concerns. To do this, it needs to promote the economic competitiveness of European seaports and related logistics.

6.2 Responsibilities

If sufficient momentum has been built towards a strategic framework, the following responsibilities would ensue:

- European Commission: collect and make available relevant EU-wide information to facilitate Member State consultations; coordinate the further development of the draft framework. Coordination would mainly lie with the Directorate-General for Mobility and Transport (DG MOVE).
- Member State governments: appoint formal contact points per Member State, and consult with each other and other relevant parties regarding the purpose, main principles and content of the draft framework.
- Sector stakeholders, including port authorities, logistical service providers (transport, terminal management, storage): participate in consultations, share best practices.

A similar approach can be taken as the EU framework for the screening of foreign direct investment to convince Member States to join, where the European Commission takes a coordinating role while autonomy remains with the Member States.

Ideally, the resulting strategic framework would be implemented through an EU regulation, similar to the FDI Screening Regulation. This would mean that all Member States across the EU are required to apply the legislative act. However, should it prove difficult to convince Member States – or the European Commission – to support a framework, this might be a step too far. In that case, the governments seeking a framework should work towards a directive

that allows individual countries to choose how to achieve the goal set out in the directive. There would be a risk that countries do not want to or cannot individually address the concerns related to foreign involvement and strategic autonomy in their legislation. The same would hold for an EU recommendation, which would be non-binding and would have no legal consequences. However, a recommendation or directive could be a first step towards stricter legislation.

6.3 Possible obstacles to implementing the framework

- Disagreement about the scope of the framework: EU Member States might have different ideas about the desired scope of the framework, and seek to broaden or narrow it.
- Commercial actors in the maritime-logistic sector might be opposed to the framework, fearing it could negatively impact the business or the investment climate.
- There are diverging interests within and among EU Member States concerning foreign involvement in maritime-logistics.
- Many EU Member States are reluctant to accept decreased national autonomy in relation to the EU-level.
- If the implementation of an EU-wide strategic framework results in limitations that specifically affect Chinese interests, the Chinese government might respond with countermeasures against EU actors.

6.4 Windows of opportunity

There are several windows of opportunity to realise the strategic framework:

- There is growing attention for foreign involvement in European seaports and logistics, from several perspectives: economic security, foreign influence and dependencies, and energy security.
- The previous European Commission recognised the need for strategic autonomy and for more efforts to deal with foreign involvement, as demonstrated by efforts towards the Economic Security Strategy and the discussion of the EU-China Strategy. The new Commission, led by Von der Leyen, is likely to continue this approach, but needs to be convinced of the added value of a strategic framework.

- The European Parliament is pushing the EU for a more strategic approach towards European seaports and logistics, with several resolutions recently passed.
- There is increasing collaboration with strategic partners, for example through the NATO Resilience Committee Transport Group.

In the light of these opportunities and obstacles, the EU and its Member States should build a **narrative** linked to the framework that emphasises that:

- the framework is country-agnostic (in combination with developing a strategic framework that indeed is not targeted at any particular country);
- the framework will increase strategic autonomy through greater insight into foreign involvement and related risks in the EU;
- this will subsequently make it easier to manage and control foreign influence and risks, and increase resilience against the disruption of critical infrastructure;
- the framework will not hinder the competitiveness of the European maritime-logistic sector, nor fully close off the maritime-logistic sector;
- rather, European cooperation will provide leverage to negotiate a more level playing field abroad;
- the framework will work best if it remains focused on maritime-logistics, instead of watering it down by broadening the scope.

7 Conclusions and recommendations

7.1 Conclusions

In order to address the consequences of foreign involvement for European seaports and related logistics it would serve the interests of the EU and its Member States to develop a **common strategic approach**. This report presents a preliminary conceptualisation of a **strategic policy framework**. While based on the relevance of China as a major player in the maritime logistical domain, the conceptualisation itself is intended to be **country-agnostic** and requires additional research to test it against case studies of countries other than China. Other non-EU actors relevant to the functioning of EU seaports and maritime logistics include Russia, the United States, the United Kingdom, Turkey, Saudi-Arabia, the United Arab Emirates, India, and Japan. Non-EU countries with complementary or competing seaports such as Egypt, Morocco and Algeria should also be taken into account.

The involvement of **foreign companies in EU ports** combined with the rapid increase in **digitisation** is driving the need for a **common European approach to data security**. This goes beyond the need to protect the integrity of individual ports. The EU as a whole is dependent on having efficient seaports whose functioning is not controlled by third countries. Likewise, there is a shared interest across the EU in the Union having competitive ports and logistical companies that benefit from trade flows, investments and technology from third countries as much as is possible without harming the **national security or strategic autonomy** of the EU or its Member States.

A common approach is needed to prevent foreign companies and governments from **pitting individual EU countries against each other**, and to share information and data among the Member States. A strategic approach to foreign involvement in seaports and logistics is necessary because of the **strategic importance of the sector**. This approach is both **more focused** than the European Commission's proposed strategy on economic security and broader than only an enhanced approach to foreign direct investment screening.

For an effective EU-wide approach to foreign involvement in European seaports and logistics, it is important to recognise that **positions and risk perceptions vary across Member States**. The strategic framework should stimulate the convergence of standards and policies and help build a common understanding of what is at stake. This requires a centralised monitoring of relevant information and sharing that information with all Member States, as well as consultations among relevant actors about the overall aims of an EU-wide strategic approach. While growing security concerns relating to foreign influence are a major driver for such an approach, such concerns should not be prioritised by default.

The matter of how to **balance security and economic interests** should remain subject to careful consideration, and is therefore a core element of the strategic policy framework.

7.2 Question 1: influencing future scenarios

*To what extent can the Dutch government or the European Union **actively influence the scenarios** mentioned in the previous report ('Navigating an uncertain future') instead of merely reacting to them?*

Individual Member States and the EU as a whole **can** actively influence future scenarios by managing the degree of foreign involvement in European seaports and logistics, with special attention for Chinese influence. However, the current toolbox of instruments does not appear to be used to its fullest extent by the Member States to protect European strategic autonomy in ports and maritime logistics. This limits control over future scenarios.

A **shared European vision** is needed on the desired level of influence. The proposed strategic policy framework supports this objective. It will maximise the use of existing instruments, and will improve upon the current tool box. The **Dutch government can lead efforts** to further realise this draft framework (see Recommendations).

7.3 Question 2: bridging differences between EU Member States

How can the strategic policy framework help bridge differences in the positions and interests among EU Member States in relation to foreign involvement in seaports and logistics?

The EU and its Member States should build on the bilateral explorative sessions already organised by the Dutch government with several Member States. From these sessions and the expert interviews conducted for this research, it was clear that while some countries are not proactive towards EU policymaking, they would **welcome** European initiatives.

Furthermore, the framework can **capture different positions** by focusing not only on risks to strategic autonomy but also on economic impact (See Figures in Chapter 4). This can help bring Member States on board that have lower threat perceptions of foreign involvement, but seek cooperation for other reasons such as economic impact.

The framework may function in a similar way as the coordination framework for **FDI screening** that became operational in 2020: the framework provides for a better overview of relevant developments and a set of commonly accepted principles and standards, while Member States retain their autonomy.

7.4 Question 3: the necessary policy instruments

Which policy instruments are needed (what is already covered by existing instruments and where are there still gaps), both at the EU and Member State level, to enable European authorities to align foreign involvement in European seaports and logistics with the aim of strategic autonomy?

Chapter 3 analysed the existing and missing policy instruments in the current toolbox. The strategic framework would bring added value by improving the (implementation of the) existing toolbox, by addressing:

- the current lack of a **focused European approach** to seaports and logistics
- **EU and Member State competition regulation**, concerning **vertical integration** and the need to be able to block or limit mergers, to limit power of companies throughout the supply chains, and with regard to their peer competitors for horizontal market power. The EU should focus specifically

on the effect of concentrations of state-owned market power on the EU's channels for external trade as a whole
- **Lack of contingency plans and intervention capabilities** based on national security to take control of strategic port or logistical companies if needed, for instance in case of a national security emergency
- **Risks in software**, technology and digital infrastructure
- the lack of a **centralised source of information**, monitoring and information sharing on foreign involvement
- **Member State FDI screening**: public transparency requirement for foreign direct investors in EU port infrastructure and transport companies.

7.5 Recommendations

- The EU's Member States and the European Commission should develop a **strategic policy framework** to address and manage foreign involvement in the EU's seaports and related logistics. The present report offers a preliminary conceptualisation of such a strategic framework.

- A primary function of the framework should be to work towards a **coherent EU-wide approach to foreign involvement** in the EU's seaports and logistics that reduces risks as much as necessary, while maintaining the benefits of foreign involvement as much as possible.

- The design and functioning of the strategic policy framework should be based on a shared understanding that across Member States there are **different economic interests and threat perceptions** relating to foreign involvement in seaports and related logistics. The strategic policy framework should facilitate a process of convergence of views regarding the desired balance between limiting the risks and maintaining the benefits of foreign involvement.

- **Key policy instruments** for the EU to manage foreign involvement in seaports and logistics include:
  - coordinated foreign direct investment screening
  - competition regulation that limits concentrations of both commercial and political power within supply chains
  - a policy to create and secure an EU-wide platform for port data.

- The framework should **address risks in the software domain**. Instruments to address risks in the software domain are:
  - Safety measures of all seaports in EU-countries must meet basic minimum requirements. This relates to port community systems and container terminals. This means attention for outdated IT-systems and regular updates and maintenance of systems.
  - Support the introduction of federated information systems. These systems make data available in an authorised manner and should be used for data traffic in intra-European port networks.
  - Use European cloud-services for the storage of vital trade data.

- All Member States and the European Commission should appoint or set up a **central point of contact** for all matters concerning foreign involvement in the EU's seaports and related logistics. The latter includes logistical systems that connect inland regions to seaports.

- The Member States and the European Commission should establish a **centralised system for gathering and sharing information** on foreign involvement in the EU's seaports and logistics.

- **The Netherlands should play a leading role** in EU-wide cooperation to discuss the introduction of the proposed strategic framework. It is well positioned because of its expertise with both the maritime logistics hub function and with policy analysis relating to strategic autonomy. In general, it is one of the few European countries with both significant public concern for dependence on China, as well as a significant prioritisation of the issue in policymaking.[99] The current level of Chinese influence in Dutch maritime logistics and infrastructure, and the strong maritime trade linkages with China, further provides incentive towards action. Moreover, the Netherlands already takes an active approach to policymaking at the EU-level and can help mobilise less active Member States. In addition, the Netherlands can share its best practices concerning its port community system, as one of the few countries with its own system. This addresses one of the high-risk areas identified in the strategic framework.

99 John Seaman, Francesca Ghiretti, Lucas Erlbacher, Xiaoxue Martin & Miguel Otero-Iglesias, "Dependence in Europe's Relations with China: Weighing Perceptions and Reality", A report by the European Think-tank Network on China (ETNC), April 2022.

- The Dutch government should build support for a common strategic framework by **engaging with other Member States**. It should do so in close cooperation with other countries (such as Poland and Belgium) that are concerned about the security implications of foreign involvement in seaports and related logistics and that feel an urgency to act at the EU level. Building support further involves an approach that appeals to the different categories of countries: (b) countries (such as France and Germany) that currently do not feel an urgency to act at the EU level, (c) countries (such as Italy, Spain and Greece) that do not regard involvement by external actors as a serious security issue; and landlocked countries.

- To get countries on board that do not regard involvement by China or other external actors as a serious risk, such as some in the Mediterranean, it is important that the Dutch government and other actors supportive of a strategic framework emphasise not just the EU-wide importance of a joint approach to risk management, but that they **also address concerns that these countries have regarding competition from ports in North Africa and the costs involved in addressing potential security risks**.

- The EU should **require reciprocity** with regard to access to the different elements of the maritime logistics hub function in third countries. This includes ports/hinterland maritime operations infrastructures, maritime support activities and regional infrastructures as well as hardware, software and orgware. The focus should be on observable outcomes, including regulatory and non-regulatory barriers.

- The strategic framework should **align with existing fora** and involve the Cybersecurity Working Group of the European Coast Guard Functions Forum (ECGFF), and formalise efforts towards information-sharing on software and cybersecurity. The strategic framework should also be discussed in other maritime European fora, such as ESPO or FEPORT.

- **Clear communication** of the framework is needed, both within the EU to get Member States on board, and outwards to reduce potential worries about the framework.

- Use the strategic framework to agree on the EU's **red lines** concerning foreign involvement in maritime logistics and infrastructure; for example on what can have private or public ownership.

- Focus the framework not only on addressing security risks but also on finding a **balance between the risks and benefits of foreign involvement**. Efforts to 'de-risk' specific economic relations with external actors such as China should be embedded in a broader strategy that helps assess which risks are unacceptable, and which are acceptable given the benefits of economic interaction.

- **Further research** on the segments of the maritime logistics hub function, identified in Chapter 5, where there currently is not enough information to assess the risks of foreign involvement to strategic autonomy.

- **Further research** to test the country-agnostic features of the framework through applications to significant non-EU countries that may pose threats to strategic autonomy and to Member States that differ structurally from those with large maritime logistics infrastructures, such as the Netherlands or Belgium.

- **Further research** is important to understand the positions and interests of the remaining 19 Member States that were not covered in this report, and to assess how the findings of this report relate to the foreign involvement of non-EU actors other than China.

Appendix A: List interviewees

Name	Position Organisation
EU DG Move	EU DG Move (written answer)
Anonymous	Representative of a large Container Terminal Operator in Europe
Anne-Marie Dedene	PHD Student, Vrije Universiteit Brussel
Jens Eskelund	Chief Representative, Maersk China Ltd.
Antoine Frémont	Professor, Conservatoire National des Arts et Métiers (CNAM)
Francesca Ghiretti	(former) Analyst, Mercator Institute for China Studies (MERICS)
Jacob Gunter	Lead Analyst, Mercator Institute for China Studies (MERICS)
Jakub Jakóbowski	Head China Department, Centre for Eastern Studies (OSW)
Olaf Merk	International Transport Forum, Organisation for Economic Cooperation and Development (OECD)
Miguel Otero-Iglesias	Senior Analyst, Elcano Royal Institute
Tim Ruhlig	Senior Research Fellow, German Council on Foreign Relations (DGAP)
Isabelle Ryckbost	The European Sea Ports Organisation (ESPO)
Yvo Saanen	Portwise
Plamen Tonchev	Head Asia Unit, Institute of International Economic Relations
Larissa van der Lugt	Erasmus Centre for Urban, Port and Transport Economics (UPT)
Marten van der Velde	Portbase

Appendix B: Overview EU instruments relevant to foreign involvement in European seaports and related logistics

Table 4 Existing EU Instruments relevant to foreign involvement in European seaports and logistics

Instrument	Economic Security Strategy[100]
Objective	"Sets out a common framework for achieving economic security by promoting the EU's economic base and competitiveness; protecting against risks; and partnering with the broadest possible range of countries to address shared concerns and interests."[101] Relevant features include a proposed reform of the Regulation on the screening of Foreign Direct Investment, and assessment of risks to economic security. Outbound investment screening is under discussion.
Status	20 June 2023: Joint Communication on a European Economic Security Strategy. 24 January 2024: EC adoption of initiatives to strengthen economic security.
Status	11 October 2020: application of the regulation. 24 January 2024: EC proposal for a revision of the Regulation on the screening of Foreign Direct Investment. It seeks to close gaps in the current mechanism, for instance by ensuring all EU Member States have a screening system and by facilitating convergence of national systems.
Instrument	**Directive on the Resilience of Critical Entities (CER) (Directive (EU) 2022/2557)[102]**
Objective	"To strengthen the resilience of critical entities against a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage, as well as public health emergencies."[103] Relevant features include the need for Member States to develop national strategies and risk assessments to identify critical entities.
Status	16 January 2023: directive entered into force. 17 October 2024: transposal into national legislation by Member States. 18 October 2024: application of the regulation (planned).

100 European Commission, "An EU approach to enhance economic security", June 2023.

101 Ibid.

102 The European Parliament and the Council of the European Union, "On the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC", December 2022https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

103 European Commission, "Critical Infrastructure Resilience", July 2024.

Instrument	Network and Information Directive (NIS2) (Directive (EU) 2022/2555)[104]
Objective	"Provides legal measures to boost the overall level of cybersecurity in the EU."[105] Relevant features include a Cooperation Group to support strategic cooperation and information exchange among Member States, and cybersecurity requirements for operators of essential services.
Status	16 January 2023: directive entered into force. 17 October 2024: transposal into national legislation by Member States. 8 October 2024: application of the regulation (planned).
Instrument	**Foreign subsidies Regulation (FSR) (Regulation (EU) 2022/2560)[106]**
Objective	"enables the Commission to address distortions caused by foreign subsidies, allows the EU to ensure a level playing field for all companies operating in the Single Market, while remaining open to trade and investment."[107] Relevant features include granting the EC the power to impose measures to redress the distortive effects of financial contributions granted by non-EU governments.
Status	12 July 2023: application of the regulation.
Instrument	**Anti-Coercion Instrument (ACI) (Regulation (EU) 2023/2675)[108]**
Objective	"to deter and respond to economic coercion, and thereby better defend its [EU] interests and those of its Member States on the global stage."[109] Relevant features include potential countermeasures to respond to economic coercion, including restricting access to foreign direct investment.
Status	27 December 2023: instrument entered into force.
Instrument	**Consortia Block Exemption Regulation (CBER)**
Objective	"allows, under certain conditions, liner shipping operators to cooperate for the provision of joint services."[110]
Status	25 April 2024: expiration CBER, after which consortia are subject to the EU antitrust rules that apply to all economic sectors.

104 European Commission, "Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive)", December 2022.
105 European Commission, "Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive)", December 2022.
106 The European Parliament and the Council of the European Union, "On Foreign Subsidies Distorting the Internal Market", December 2022.
107 European Commission, "Foreign Subsidies Regulation", accessed August 2024.
108 The European Parliament and the Council of the European Union, "On the Protection of the Union and its Member States from Economic Coercion by Third Countries", November 2023.
109 European Commission, "New tool to Enable EU to Withstand Economic Coercion Enters Into Force", December 2023.
110 European Commission, "EU competition law – evaluation of the Consortia Block Exemption Regulation", accessed August 2024.

Instrument	Horizontal Co-operation Agreement (OJ C 11)[111]
Objective	"intended to provide legal certainty by assisting undertakings to assess the compatibility of their horizontal cooperation agreements with Union competition rules while ensuring effective protection of competition. They also aim to make it easier for undertakings to cooperate in ways which are economically desirable, thereby contributing, for example, to the green and digital transitions and to promoting the resilience of the internal market."
Status	21 July 2023: Revised Horizontal Guidelines.[112]
Instrument	**Revision of TEN-T Regulation 2013 (2021/0420(COD))[113]**
Objective	"To support the transition to a cleaner, greener and smarter mobility in line with the European Green Deal and the Sustainable and Smart Mobility Strategy."[114]
Status	14 December 2021: EC made initial legislative proposal to revise TEN-T regulation. July 2022: EC made amended proposal in reaction to Russia's war of aggression. June 2024: entered into force.[115]
Instrument	**European Ports Alliance[116]**
Objective	"to step up the fight against drug trafficking and organised crime. This partnership aims to bring all relevant stakeholders together, to form solutions to protect ports."[117] Relevant features include the creation of a Public Private Partnership to strengthen the resilience of ports and stepping up the fight against drug trafficking and criminal infiltration.
Status	24 January 2024: launched by the European Commission, together with the Belgian Presidency of the Council of the EU.[118]

111 European Commission, "Communication from the Commission: Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements", January 2011.

112 European Commission, "Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements", June 2023.

113 European Commission, "Regulation of the European Parliament and of the Council: on Union Guidelines for the Development of Trans-European Transport Networks, Amending Regulations (EU) 2021/1153 and Regulation (EU) No 913/2010 and repealing Regulation (EU) 1315/2013", December 2021.

114 European Commission, "Trans-European Transport Network (TEN-T)", accessed August 2024.

115 Legislative Observatory (EU), "2021/0420(COD): Trans-European Transport Network", January August 2024.

116 European Commission, "European Ports Alliance to Fight Drug Trafficking and Organised Crime", January 2024.

117 Ibid.

118 European Commission, "Commission Launches the European Ports Alliance Public Private Partnership to Fight Organised Crime and Drug Trafficking", January 2024.

Instrument	Revised EU Maritime Security Strategy (EUMSS)[119]
Objective	"framework for the EU to take further action to protect its interests at sea, and to protect its citizens, values and economy. The aim is to promote international peace and security, as well as safeguard free flow of trade and freedom of navigation, while adhering to the principle of sustainability and protecting biodiversity." Relevant features include the commitment to manage risks and threats and to cooperate with partners to protect EU fundamental interests.
Status	24 October 2023: approved by the Council of the EU.[120]
Instrument	**AI Act (Regulation (EU) 2024/1689[121]**
Objective	"to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union."[122]
Status	1 August 2024: regulation entered into force. 2 February 2025: prohibitions and general provisions apply. 2 August 2026: most articles including obligations for high-risk AI in force. 2 August 2027: obligations for high-risk AI systems in products in force. 2 August 2030: obligations for AI systems used by government organisations that were already in use before entering into force.

119 European Commission, "Maritime Security Strategy", accessed August 2024.

120 Council of the EU, "Maritime Security: Council Approves Revised EU Strategy and Action Plan", October 2023.

121 European Commission, "Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)", June 2024.

122 Ibid.