IN-DEPTH ANALYSIS

Requested by the SEDE sub-committee

European Parliament

Security implications of China-owned critical infrastructure in the European Union

Author:
Frank JÜRIS

European Parliament coordinator:
Policy Department for External Relations
Directorate General for External Policies of the Union

PE 702.592 - June 2023

EN

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

European Parliament

IN-DEPTH ANALYSIS

Security implications of China-owned critical infrastructure in the European Union

ABSTRACT

China's footprint in European critical assets has grown steadily over time, without any centralised mechanism that could give the European Union (EU) and Member State agencies visibility and scrutiny over projects of strategic significance for Europe's defence and security. China's footprint poses specific challenges to Europe's efforts to protect its critical infrastructure. China's party-led political system does not allow clear distinctions between commercial, political and military interests, often viewing Chinese state and private companies' international activities as instruments helping the Chinese Communist Party (CCP) expand its influence in foreign countries and undermine geopolitical rivals. The CCP's military-civil fusion (MCF) strategy incentivises civilian actors to contribute to the modernisation of the People Liberation Army (PLA) through technology transfer. Chinese companies' access to EU critical infrastructure thus calls for an analysis of threats to Europe's defence and security architecture. Using research with original Chinese-language sources, this paper analyses the involvement of China state-linked entities in selected critical sectors — ports, rare metals and undersea cables — to identify short-, medium- and long-term threats to the EU's strategic sovereignty. These cases expose how entities linked to the Chinese party-state can gain access to and exert influence on assets that are vital to Europe's security and defence, including transport infrastructure, critical resources and telecommunications networks. This research demonstrates that traditional approaches to infrastructure protection based on direct ownership are insufficient, since China's party-state can obtain access to critical infrastructure through indirect, equally effective channels. As these cases show, infrastructure protection mechanisms, whose codification and implementation remains incomplete, must be extended to be able to scrutinise the risks that China's leverage over non-science investors and Chinese state-linked contractors pose to the EU's critical infrastructure.

EP/EXPO/SEDE/FWC/2019-01/LOT4/3/C/15
June 2023 - PE 702.592

EN

Policy Department, Directorate-General for External Policies

AUTHOR

- Frank JÜRIS, Researcher International Centre for Defence and Security (ICDS), Estonia

The author would like to thank Jichang Lulu (Independent researcher), Filip Jirouš (Independent researcher), Tetiana Fedosiuk (Publications and Events Assistant at ICDS) and Rüüt Kaljula (Research Fellow at ICDS) for their research assistance and editing.

PROJECT COORDINATOR (CONTRACTOR)

- Trans European Policy Studies Association (TEPSA), contractor

This paper was requested by the European Parliament's sub-committee on Security and Defence (SEDE).

CONTACTS IN THE EUROPEAN PARLIAMENT

Coordination: Jérôme LEGRAND, Policy Department for External Relations

Editorial assistant: Grégory DEFOSSEZ

Feedback is welcome. Please write to jerome.legrand@europarl.europa.eu

To obtain copies, please send a request to poldep-expo@europarl.europa.eu

VERSION

English-language manuscript completed on 23 June 2023.

This paper is published on the European Parliament's online database, 'Think Tank'

Table of contents

List of abbreviations

ASN	Alcatel Submarine Networks
BRI	Belt and Road Initiative
CER	Critical Entities Resilience Directive
CCP	Chinese Communist Party
DoD	Department of Defense
EU	European Union
FDI	Foreign Direct Investment
FSR	Foreign Subsidies Regulation
FCC	Federal Communications Commission
ICTs	Information and Communication Technologies
MEP	Member of the European Parliament
MCF	Military-Civil Fusion
MSR	Maritime Silk Road
NATO	North Atlantic Treaty Organisation
NSIA	National Security and Investment Act
NISEC	Information Security Engineering Technology Center
NPM	Neo Performance Materials
PLA	People's Liberation Army
PLAN	People's Liberation Army Navy
US	United States
USA	United States of America

List of tables

1 Introduction

Since 2019, the European Union (EU) has simultaneously regarded China as a partner, a competitor and a systemic rival[1]. However, the relationship between the EU and China has worsened over time. China's human rights abuses in Xinjiang resulted in the EU imposing sanctions on Chinese officials responsible for these violations. China has retaliated with unfounded countersanctions on Members of the European Parliament (MEPs) and China scholars, which disrupted discussions on the Comprehensive Agreement on Investment. Lithuania, as the first EU Member State to withdraw from China's '16+1' format and to open a representative office in Taiwan in recent years, was imposed unofficial sanctions on from China. These sanctions prompted the EU to take action, which requested the intervention of a World Trade Organization's panel to address the issue: '… the EU is protecting its Member States against China's discriminatory measures, which the EU considers to be in breach of WTO [World Trade Organization] rules[2].'

China's oppressive domestic policy and assertive foreign policy have led critical voices in the EU to propose a revaluation of the EU's China policy with an emphasis on competition and rivalry[3]. According to High Representative of the EU for Foreign Affairs and Security Policy, Josep Borrell Fontelles: 'Its [China's] ambition is clearly to build a new world order, with China at the centre, becoming by the middle of the century the world's leading power'[4]. To mitigate risks Borrell proposed a recalibrated stance on economic security, stating that 'a more effective export control system, the control of inbound investment and possibly outbound investment, and the smart use of the anti-coercion instrument[5].' Borrell's proposal echoed Commission President Ursula von der Leyen's earlier formulation of economic de-risking from China by enhancing Europe's competitiveness, improving and implementing existing toolboxes and trade instruments, developing defence measures for avoiding sensitive technologies transfer to China and alignment with likeminded partners to better deal with shared concerns[6].

1.1 China's political system's challenges to critical infrastructure protection

China's party-state and its international projection pose unique challenges to critical infrastructure-protection frameworks. Unlike democratic nations, in China's party-driven political system and economy, distinctions between state and private entities alongside commercial, political and military interests are blurred. Regulatory requirements and uncodified relationships with state agencies often bind private companies to align their commercial interests with the Chinese Communist Party's (CCP) defence, repression and political interference initiatives. These initiatives treat Chinese companies' international activities as instruments helping the party expand its influence on foreign countries and undermine geopolitical rivals. Under President Xi Jinping, the party-led system increasingly incentivises civilian actors to contribute to the People Liberation Army's (PLA) modernisation through technology transfer. An analysis of risks emanating from Chinese entities' investment in and access to European critical infrastructure thus necessitates understanding those entities' relationship with the CCP and its policies.

[1] Joint Communication to the European Parliament, the European Council and the Council. EU-China – A strategic outlook, JOIN (2019) 5 Final, 12 March 2019.
[2] European Commission, 'EU requests two WTO panels against China: trade restrictions on Lithuania and high-tech patents', IP/22/7528, 7 December 2022.
[3] A. Brzozowski, 'EU expected to take a tougher stance on China', *Euractiv*, 17 October 2022.
[4] J. Borrell, 'How to deal with China', *European External Action Service*, 17 May 2023.
[5] J. Borrell, 'How to deal with China', *European External Action Service*, 17 May 2023.
[6] European Commission, 'Speech by President von der Leyen on EU-China relations to the Mercator Institute for China Studies and the European Policy Centre', SPEECH/23/2063, 30 March 2023.

The entanglement between Chinese private commercial interests and CCP policy increasingly impacts the EU and its Member States' handling of China's access to European critical infrastructure, with the telecommunications sector providing key examples. EU agencies and Member States have proposed the exclusion of Chinese private businesses, for example, Huawei and ByteDance, from accessing sensitive assets, such as infrastructure projects or government devices.

The integration of large private enterprises into the party-state's defence and security apparatus entails that China's private sector's access to European critical infrastructure potentially transfers that access to the party-state itself. Under General Secretary Xi Jinping, the CCP has made Military-Civil Fusion (MCF, 军民融合) a 'national strategy'[7]. MCF, whose conceptual roots trace back to the Mao era, goes beyond traditional concepts of 'dual-use' technology to mandate multiple agencies capable of integrating civilian as well as military research and development. Specifically, it incentivises private businesses and civilian universities to contribute to military development[8]. Intelligence agencies also have close links with private companies that have made inroads into EU Member States. For instance, CEFC China Energy, a defunct energy company that became prominent as an investor cultivating links in the Czech Republic, was linked to one of China's military intelligence agencies through various figures, including its chairman[9]. Huawei, excluded from many EU projects on account of its state ties, also has personnel links to the Ministry of State Security, China's main civilian intelligence agency[10].

Chinese investment leads to further entanglements between the party-state and European stakeholders that go beyond direct threats to critical infrastructure. The EP's Special Committee on Foreign Interference in all Democratic Processes in the EU, including Disinformation has identified 'elite capture', where China and other authoritarian actors establish 'channels of influence' by co-opting key European stakeholders. This is a foreign interference risk area that the EU is currently ill equipped in[11]. When Chinese state-linked entities become key actors in Member-State economies, for instance by investing or promising to invest in infrastructure projects or building or maintaining them as contractors, channels to influence decision-makers and local businesses are created. Even without actual economic benefits for target countries, the Chinese government exploits perceptions of potential trade and investment to coax foreign states' policies into alignment with the CCP's geopolitical goals. As an example, this can be seen in some States' adherence to CCP geopolitical initiatives, such as the Belt and Road Initiative (BRI) or the '16+1' format[12], despite a near total absence of benefits to their economies. While nations influencing each other's behaviour is a common aspect of international relations, China's Leninist system comprises an extensive bureaucracy heavily involved in political influence operations. Originally copied from the Soviet Union and with few modern parallels outside Russia, these activities, along with civilian and military intelligence agencies, engage in party and state propaganda, foreign affairs, united front, commerce and other organs.

[7] People's Daily, '习近平：深入实施军民融合发展战略 努力开创强军兴军新局面' , 13 March 2015 [web archive].
[8] A. Stone and P. Wood, China's Military-Civil Fusion Strategy: A View from Chinese Strategists, China Aerospace Studies Institute; A. Fritz, 'The foundation for innovation under military-civil fusion: The role of universities', *Sinopsis*, 8 October 2021.
[9] M. Hála, 'United Front Work by Other Means: China's "Economic Diplomacy" in Central and Eastern Europe', *Jamestown Foundation*, China Brief, Vol 19, No 9, 9 May 2019; M. Stoke and R. Hsiao, 'The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics', *Project 2049 Institute*, 14 October 2013.
[10] *Open Source Center*, Huawei Annual Report Details Directors, Supervisory Board for First Time, 5 October 2011; M. Hála, Jichang Lulu, 'Huawei's Christmas battle for Central Europe', *Sinopsis*, 28 December 2018.
[11] European Parliament, Report on foreign interference in all democratic processes in the European Union, including disinformation, Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, 2020/2268(INI), 8 February 2022.
[12] The 16+1 cooperation format was launched by China in 2012. It originally engaged 16 Central and Eastern European countries, including 11 EU Member States. Three states have subsequently abandoned the format, while others have effectively suspended any active participation.

1.2 The EU and Member States' capabilities to protect critical infrastructure

Recent European Commission directives have identified, as part of critical infrastructure, key assets that are vital in the provision of essential services, ranging from energy and transport to digital connectivity. Threats to such infrastructure are, directly or indirectly, threats to the security and defence capabilities of the EU Member States. The European Parliament (EP) has introduced regulations that call for special attention to be paid to critical infrastructure within foreign direct investment (FDI) screening procedures. This framework provides the EU agencies and Member States with tools to scrutinise non-EU investment in critical assets, including activity by China. While aspects of this framework are premised on non-discrimination between third countries, specific EU measures, such as sanctions against human-rights abuses in Xinjiang, have specifically targeted Chinese entities. This framework does not, however, endow EU agencies with decision-making powers, thus leaving the actual codification and enforcement of screening mechanisms up to Member States. Although these agencies can scrutinise non-EU involvement in critical infrastructure, albeit still short of enforcement, such scrutiny is not currently carried out systematically. No due diligence and active scrutiny schemes are currently in place that would allow EU agencies to identify Chinese and non-Chinese actors' vulnerability to the Chinese party-state's influence on European critical infrastructure. While an evolving regulatory framework addresses FDI, no similar mechanism appears to exist at EU level to scrutinise China's access to critical infrastructure through channels other than direct investment.

The EU's regulatory framework defines concepts of critical infrastructure and strategic resources that are of relevance to Europe's defence and security. The EP's Critical Entities Resilience (CER) Directive of December 2022 defines critical infrastructure as 'an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service'. The same directive defines essential services as those 'crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment'[13]. The Network and Information Security 2 (NIS2) Directive adopted in January 2023 made explicit the critical nature of communications infrastructure, stating that 'Member states should ensure that the security of the public electronic communications networks is maintained and that their vital security interests are protected from sabotage and espionage' and in particular '[t]he national cybersecurity strategy should, where relevant, take into account the cybersecurity of undersea communications cables'. Hostile action targeting these systems would significantly compromise Member States' defence capabilities.

Although those directives show evolving EU efforts to protect critical infrastructure, the actual codification of such initiatives remains largely restricted to one aspect of protection, namely that involving foreign direct investment. However, even here such efforts face implementation limitations. While EU-level regulation provides broad guidance on FDI-screening procedures, their implementation remains the task of Member States and is therefore subject to local approaches. FDI Regulation EU 2019/452 introduced procedural baseline standards, guidance on matters related to the national security interest and a cooperation mechanism[14]. The Foreign Subsidies Regulation (FSR) EU 2020/2569[15] supplemented the regulatory framework, imposing compliance obligations on foreign subsidies. As the case studies in this report will show, the combination of this EU-level guidance with Member States' actions does not yet

[13] See Article 2. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance), Official Journal of the European Union, L 333/164, 27 December 2022.
[14] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, Official Journal of the European Union, LI 79/1, 21 March 2019.
[15] Regulation (EU) 2022/2560 of the European Parliament and of the Council of 14 December 2022 on foreign subsidies distorting the internal market, Official Journal of the European Union, L 330/1, 23 December 2022.

consistently react to investments in critical infrastructure, even when their potentially threatening nature becomes a topic of public debate.

Beyond direct investment, EU and Member State measures have targeted specific Chinese companies whose access to critical infrastructure was deemed a threat, demonstrating current frameworks' ability to differentially address the risks posed by different states beyond a general framework. In particular, some of these measures have sought to reduce the footprint that Chinese companies linked to China's party-state and intelligence apparatus have in the EU's telecommunications infrastructure. Various Member States have employed a variety of mechanisms to limit the party, military and intelligence-linked company Huawei's participation in the EU's 5G networks[16]. Member States and EU agencies have also banned or warned against the use of a content-sharing application developed by ByteDance, a Chinese firm linked to the party and its propaganda efforts[17].

The EU's Global Human Rights Sanctions Regime further shows Europe's capability to target China's security system for its responsibility in political surveillance and repression activity. In 2021, the EU imposed sanctions on security officials involved in repression against Uyghurs and others in China's Xinjiang Uyghur Autonomous Region. China's security apparatus's surveillance role directly translates into threats to Europe's security when Chinese entities with security links gain access to critical infrastructure. However, the current regulatory framework does not reflect this key link between domestic human rights violations and the global extension of China's surveillance and intelligence apparatus[18].

These measures and regulatory efforts illustrate EU agencies as well as Member States' ability and willingness to respond to threats posed by entities linked to the Chinese party-state. However, they also indicate that a unified framework must be put in place which can provide effective protection for Europe's critical infrastructure. Consistent regulatory guidance is taking shape only on FDI, which, as case studies below will demonstrate, is only one channel through which the Chinese party-state may gain access to and influence critical assets. Member States' response to party-state-linked threats has been triggered solely in isolated, well-publicised cases such as Huawei and ByteDance. This points to a lack of proactive scrutiny regarding China's leverage on infrastructure projects.

1.3 Previous research on Chinese FDI in Europe

China's investment in the EU, including critical infrastructure, has received increasing attention over recent years from academic and think tank scholars. Germany-based think tank MERICS and economic research firm Rhodium Group have since 2015 jointly published annual comprehensive EU-wide and sector-based overviews of Chinese FDI in Europe[19]. The US think-tank German Marshall Fund's 2021 report on Chinese FDI in European infrastructure highlighted the importance of taking an aggregate approach in analysing

[16] On Huawei's links to the party, the army and the intelligence apparatus, see F. Jirouš and J. Lulu, 'Huawei in CEE: From "strategic partner" to potential threat', *Sinopsis*, 17 May 2019; K. Kono and S. De Tomas Colatin. 'National Approaches to the Supply Chain Cybersecurity: Taking a More Restrictive Stance Against High-Risk Vendors', *NATO Cooperative Cyber Defence Centre of Excellence*, 2023.

[17] On TikTok's party links, see R., Lee, P., Luttrell, M., Johnson and J., Garnaut, 'TikTok, ByteDance, and their ties to the Chinese Communist Party', *Submission to the Australian Senate Select Committee on Foreign Interference through Social Media*, 14 March 2023; European Commission, 'Commission strengthens cybersecurity and suspends the use of TikTok on its corporate devices', Press Release, 23 February 2023; *Euronews* and *Associated Press*, 'Which countries have banned TikTok and why?', 4 April 2023.

[18] Council Decision (CFSP) 2021/481 of 22 March 2021 amending Decision (CFSP) 2020/1999 concerning restrictive measures against serious human rights violations and abuses, Official Journal of the European Union, LI 99/1, 22 March 2021.

[19] T. Hanemann and M. Huotari, 'Chinese FDI in Europe and Germany Preparing for a New Era of Chinese Capital', *Mercator Institute for China Studies and Rhodium Group*, June 2015; A. Kratz, M. J. Zenglein, G. Sebastian and M. Witzke, 'Chinese FDI in Europe 2021 Update: Investments remain on downward trajectory-Focus on venture capital', *Mercator Institute for China Studies*, 27 April 2022.

decision-making within states and companies due to potential security risks[20]. Country-based case studies were presented within the European Think-tank Network's 2017 China report focusing on national-level debates on Chinese FDI[21]. Based on case studies of specific countries, the Swedish Defence Research Agency conducted a survey on the acquisition of Swedish companies by Chinese and Hong Kong firms. Results emphasised a significant connection between these acquisitions and China's national industrial development plan known as 'Made in China 2025'[22].

This analysis builds upon the existing body of research highlighting here only a few examples with shared approaches from Chinese central-level planning to EU-wide reach and granular security assessment based on Chinese actors' detailed background analysis. Valuable insights for the following case studies were derived from research commissioned by the EP's Subcommittee on Security and Defence about security threats related to undersea communication cables. Additionally, the US Naval War College has analysed China's power projection through the acquisition of commercial ports worldwide, which has also provided important information[23]. However, no comprehensive study has so far been produced detailing China's investments in and access to EU critical infrastructure, nor does this paper attempt to provide one due to time and space constraints. Previous literature often provides quantitative snapshots of China's investments, which does not yield sufficient input for any risk assessment from a defence and security viewpoint.

1.4 Scope of the research

This In-depth analysis builds on the policy and scholarly communities' previous treatments of the China infrastructure investment problem to identify lingering challenges to the EU's critical infrastructure-protection framework. Aspects of this problem have already been addressed by EU and Member-State regulatory efforts and debated in academic literature, think-tank policy briefs and media reports and commentary. A comprehensive review of China's investments in EU critical infrastructure would greatly exceed the scope of this analysis. Instead, case studies have been selected to test existing regulations against the risk profile of China's current involvement in Europe's infrastructure. To this end, the cases focus on problematic infrastructure investments that appear to show a lack of implementation *vis-à-vis* EU screening guidelines. These are investments where indirect, yet significant China leverage may by-pass current screening procedures and understudied forms of China access to critical infrastructure through channels that do not involve direct company ownership, thus challenging *any* investment-screening framework. In most cases, efforts have been made to highlight poorly known projects and risks, aiming to add to, rather than duplicate, previous literature. While the challenges identified are of cross-EU significance, the examples from the Nordic-Baltic region in some of the studies reflect the author's expertise and subjects of ongoing research. As discussed in each case, the regional examples do not distract from the continental significance of the risks studied but provide the necessary depth for analysis.

This analysis has identified serious challenges to the EU's critical infrastructure, some of which cannot be tackled directly by the current regulatory instruments. Chinese companies controlled or strongly influenced by the party-state hold significant stakes in many critical infrastructure projects. These investments largely began in a legislative vacuum before EU screening guidelines were in place. However, the fact that these processes continue in some cases suggests that the regulatory vacuum lives on: Member

[20] D. Cristiani, M. Ohlberg, J. Parello-Plesner and A. Small, 'The Security Implications of Chinese Infrastructure Investment in Europe', *The German Marshall Fund, Washington:DC*, 28 September 2021, p. 7.
[21] J. Seaman, M. Huotari and M. Otero-Iglesias, Chinese Investment in Europe: A Country-Level Approach, Report, *European Think-tank Network on China*, December 2017.
[22] J. Hellström, O. Almén, and J. Englund, Chinese corporate acquisitions in Sweden: A survey, *Swedish Defence Research Agency*, February 2021.
[23] C. Bueger, T. Liebetrau and J. Franken, 'Security threats to undersea communications cables and infrastructure – consequences for the EU', Policy Department of the European Parliament, PE 702.557, June 2022; I. B. Kardon and W. Leutert, Pier Competitor: China's Power Position in Global Ports, *International Security*, Vol 46, No 4, 2022, pp. 9–47.

States, ultimately responsible for infrastructure protection, are not consistently implementing those guidelines or setting up national-level investment-screening mechanisms. In other cases, investment screening is challenged by China's leverage on private companies from third countries. In such situations, the party-state's ability to influence an investor's decisions can create comparable risks to a direct China ownership stake. Finally, similar risks can arise from China entities' access to critical infrastructure, even when no ownership is involved. Chinese companies (some with links to the party-state and the military) have become contractors for critical infrastructure projects. While Member States may have national-level instruments to reduce that exposure to contractors, the absence of an EU-wide response shows that the screening of actors with access to critical infrastructure cannot be limited to direct investment.

This research is structured in the form of three case-study risk analyses, followed by policy implications and recommendations. The **Introduction**, based on previous research literature and policy documents, presents background on the EU approaches to the screening of China's access to infrastructure, as well as a summary of distinctive risks that emanate from the nature of China's political system. **Section 2** discusses selected Chinese investments in European ports. While many of these projects involve relatively small China-owned stakes and entail little short-term risk, the critical importance of port infrastructure for Europe's security and defence magnifies the potential impact of future espionage and sabotage. The analysis finds that, in the medium and long term, investors with Chinese state control (state-owned companies) and Chinese (including Hong Kong) private companies with indirect, yet strong party-state links can have similar risk profiles. This finding has methodological implications for screening procedures, which should analyse risks arising from political and business connections to the party-state, rather than just state ownership. **Section 3** features rare earth minerals, which the EU has identified as a critical resource, to highlight the importance of China's influence and leverage beyond direct corporate ownership. While the EU and its allies increasingly seek to achieve supply-chain resilience, the fact that major actors in the industry are vulnerable to the Chinese government's influence can negate some of those efforts; at worst, it can effectively mean EU support for the opposite of any intended goal, strengthening China's control of the global rare earths supply. The final case study, in **Section 4**, adds to active debates on 5G and other aspects of telecommunication infrastructure: undersea cables, which are essential for civilian and military communications. This analysis finds that China's entities, some with links to the Chinese defence sector and involved in military-civil fusion activities, have extensive access to undersea cable projects, as contractors. **Section 5** summarises these risks and recommends measures to mitigate them.

2 Chinese investments in port infrastructure

Chinese entities, directly controlled or strongly linked to the party-state, own stakes in various European port terminals. In some cases, these terminals are situated in logistical hubs that are key to Europe's defence, including military bases. Although current EU FDI-screening procedures would likely have objected to these investments, many were made before such mechanisms were in place or lacked the political will to implement action. Even in more recent and ongoing cases, the advisory nature of these mechanisms renders them unenforceable, creating vulnerabilities of EU-wide significance in Member States that have not yet implemented investment-screening standards.

2.1 From the maritime silk road to maritime great power

China is striving to become a leading world power by the middle of the century when the country celebrates its 100th anniversary. Central to this aim is the 'Chinese dream' of a 'great rejuvenation of the Chinese people' by which China wants to become the strongest military force on the planet. One important aspect of becoming the leading power is to have the strongest navy in the world, assisted by a fleet of

civilian vessels if necessary. Overseas ports and terminals that could host Chinese (war-) ships would play an equally important role in China projecting its power[24].

China's strive to become the leading maritime force globally was elevated into a national goal[25] in late 2012, during the 18th National Congress of the CCP, when Hu Jintao, CCP General Secretary at the time, in his last report to Congress mentioned 'building China into a maritime great power' [26]. Since then, China under President Xi Jinping has launched BRI which also has a maritime component, the '21st Century Maritime Silk Road' (MSR), a transport route reaching from the South China Sea to the waters of Europe. Chinese shipping giant **COSCO**'s takeover of the Port of Piraeus in Greece and the construction and operation of the Vado container terminal in Italy are examples of MSR activities[27]. 'The Chinese government regards the MSR as an important way to participate in international ocean governance', as covered in an article published on the Chinese government website[28]. 'International ocean governance' is defined by the European Commission as 'managing the world's oceans and their resources together so that they are healthy and productive, for the benefit of current and future generations'[29]. This article also praises cooperation between China and other countries when it comes to managing oceans: 'The roads of cooperation, prosperity, openness, greenness, win-win and integrity for the development of countries and regions along the route'[30].

China's investments in port infrastructure across the globe are driven not only by commercial but also strategic interests. In addition to buying up ports and terminals to support its trade-dependent economy, the need to keep maritime trade routes open with the help of a growing navy is noted in Chinese sources. China has fundamentally changed its military doctrines to project its naval might into the open seas. For instance, China's Military Strategy white paper, introduced in 2015, states that 'in line with the strategic requirement of offshore waters defence and open seas protection, the PLA Navy (PLAN) will gradually shift its focus from 'offshore waters defence' to a combination of 'offshore waters defence' with 'open seas protection', thereby building a combined, multi-functional and efficient marine combat force structure. The PLAN will enhance its capabilities for strategic deterrence and counterattack, maritime manoeuvres, joint operations at sea, comprehensive defence and comprehensive support'[31].

The US Department of Defense (DoD) report on China's military capabilities (2022) describes how China is:

> 'Seeking to establish a robust overseas logistics infrastructure to allow the PLA to project and sustain military power at greater distances. Beijing may assess that a mixture of military logistics models, including preferred access to commercial infrastructure abroad, exclusive PLA logistics facilities with prepositioned supplies co-located with commercial infrastructure and bases with stationed forces, most closely aligns with China's overseas logistics needs. Currently, China uses commercial infrastructure to support all its military operations abroad, including the PLA's presence in other countries' territories, such as its base in Djibouti. Some of China's BRI projects could create a potential military advantage, such as PLA access to selected foreign ports

[24] D. Thorne and B. Spevack, 'Harbored Ambitions: How China's Port Investments Are Strategically Reshaping the Indo-Pacific', *C4ADS innovation for peace*, 17 April 2018.
[25] M. Duchâtel and S.A. Duplaix, 'Blue China: Navigating the Maritime Silk Road to Europe', *European Council on Foreign Relations*, 23 April 2018.
[26] People.com.cn, '胡锦涛在中国共产党第十八次全国代表大会上的报告'，人民网，18 November 2012.
[27] Gov.cn, '共建二十一世纪海上丝绸之路'，webpage, 3 May 2015.
[28] Gov.cn, '共建二十一世纪海上丝绸之路'，webpage, 3 May 2015.
[29] European Commission, 'International Ocean Governance: an agenda for the future of our oceans', 26 February 2021.
[30] Gov.cn, '共建二十一世纪海上丝绸之路'，webpage, 3 May 2015.
[31] The State Council Information Office, 'China's Military Strategy', Ministry of National Defense of the People's Republic of China, White Paper, May 2015.

to pre-position the necessary logistics support to sustain naval deployments in waters as distant as the Indian ocean, Mediterranean Sea, and Atlantic ocean to protect its growing interest'[32].

Chinese military actively seeks to exploit civilian infrastructure for dual-use purposes. Apart from operating 'maritime militia', often blurring the lines between civilian and military vessels, the naval forces have legal tools to ensure that Chinese civilian ships and infrastructure can be used for military and security purposes. One such tool is the 2016 Law of the People's Republic of China on National Defence Transportation, which mandates that all Chinese entities abroad, including transportation companies, must 'provide assistance in the form vessels, aircraft, vehicles, personnel and resupply' for military operations, specifically 'international rescue, maritime escorting, protection of national maritime interests'[33]. According to a report citing Chinese regulations, commercial ships are often retrofitted by the state to be compatible with military specifications so that they can be used more effectively for military purposes. The report also states that civilian ships now participate more regularly in military exercises[34].

2.2 China's investments in Europe's port infrastructure

Various large Chinese shipping conglomerates have invested in ports and terminals across Europe. Three of the companies with large shareholdings in European ports are: (1) COSCO Shipping Corporation (中国远洋海运集团有限公司); (2) Hutchinson Port Holdings (Hutchinson, 和記港口集團有限公司); and (3) China Merchants Port Holdings (招商局控股港口有限公司):

(1) **China COSCO Shipping Corporation** is wholly owned by the central government[35]. This company has a well-integrated party structure as the company's senior management concurrently leads its party organisation[36].

(2) **Hutchinson Port Holdings** is a subsidiary of the Hong Kong-listed CK Hutchinson Holdings Ltd (長江和記實業有限公司)[37]. The largest beneficial shareholder (30 %) of the holding company is Li Ka-Shing (李嘉誠), a Hong Kong tycoon known for his pro-Beijing positions[38]. Furthermore, his son Victor Li Tzar-Kuoi (李澤鉅), who chairs the holding company, served between 2018 and 2023 as a member of the Chinese People's Political Consultative Conference, a top-level united front body[39].

(3) **China Merchants Port Holdings** is 65 % controlled by China Merchants Group (招商局集团), an investment company owned by the central government[40].

[32] US Department of Defense, Military and Security Developments Involving the People's Republic of China 2022, report to the Congress, 29 November 2022, p. 144.
[33] National People's Congress, '中华人民共和国国防交通法', 3 September 2016.
[34] L. D. Henley, 'China Maritime Report No. 21: Civilian Shipping and Maritime Militia: The Logistics Backbone of a Taiwan Invasion', China Maritime Studies Institute, May 2022.
[35] Baidu Aiqicha, '中国远洋海运集团有限公司', webpage, n.d.
[36] COSCO Shipping, '公司高管', webpage, n.d.
[37] CK Hutchinson Holdings, 'Ports and Related Services', webpage, 11 April 2023.
[38] CK Hutchinson Holding, Solid • Resilient Resilient Ready for Tomorrow: 2021 Annual Report, 11 April 2022.
[39] Chinese People's Political Consultative Conference, '中国人民政治协商会议第十三届全国委员会委员名单', 11 May 2020.
[40] China Merchants Port Holdings, 2021 Annual report, 2022; China Merchants Group, 'About us', webpage, n.d.

Table 1: COSCO investments in ports in Europe

Countries	Ports	Terminals	Naval bases, North-Atlantic Organization (NATO) and US Armed Forces presence
Greece	Athens	Piraeus	None
Belgium	Zeebrugge	CSP Zeebrugge	Marinebasis Zeebrugge Marinecomponent | Defensie
Spain	Valencia	CSP Valencia	US national support element Valencia, Spain, NATO rapid deployable corps, Spain
Italy	Vado Ligure	Vado Reefer	None
Italy	Vado Ligure	Vado container	None
Spain	Bilbao	CSP Bilbao	None
Belgium	Antwerp	Antwerp	US Armed Forces special agreement for transporting troops NATO in deep water because of Chinese port investments
Netherlands	Rotterdam	Euromax	Marine Corps | Royal Netherlands Navy; US Armed Forces special agreement for transporting troops NATO in deep water because of Chinese port investments
Germany	Hamburg	Container Terminal Tollerort	None

Source: COSCO Shipping, '码头组合' website.

Table 2: Hutchison investments in ports in Europe

Countries	Ports	Terminals	Naval bases, NATO and US Armed Forces presence
Belgium	Willebroek	Hutchison Ports Belgium	None
Germany	Duisburg	Hutchison Ports Duisburg	None
Poland	Gdynia	Hutchison Ports Gdynia	Seaborne Operations Center - Seaborne Component Command in Gdynia, 3rd Ship Flotilla 'Commodore Bolesław Romanowski' in Gdynia-Oksywie Jednostki podległe - 3.FO Gdynia Naval Aviation Brigade 'Commander Pilot Karol Trzask-Durski' in Gdynia, Naval hydrographical bureau in Gdynia, Diving and deep diving training Center of the Polish Armed Forces 'Commodore Stanisław Mielczarek' in Gdynia; US Armed Forces special agreement for transporting troops NATO in deep water because of Chinese port investments
Spain	Barcelona	Hutchison Ports Best	None
Sweden	Stockholm Norvik	Hutchison Ports Stockholm	Muskö naval base, near Norvik

Netherlands	Amsterdam	Hutchison Ports Amsterdam	Secondary naval base Koninklijke Marine | Defensie.nl
Netherlands	Rotterdam	Hutchison Ports ECT Delta	Marine corps | Royal Netherlands Navy; US Armed Forces special agreement for transporting troops NATO in deep water because of Chinese port investments
Netherlands	Rotterdam	Hutchison Ports ECT Euromax	Marine Corps | Royal Netherlands Navy; US Armed Forces special agreement for transporting troops NATO in deep water because of Chinese port investments
Netherlands	Rotterdam	Hutchison Ports Delta II	Marine Corps | Royal Netherlands Navy; US Armed Forces special agreement for transporting troops NATO in deep water because of Chinese port investments
Netherlands	Moerdijk	Moerdijk Container Terminals	None
Netherlands	Amsterdam	TMA Logistics	Secondary naval base Koninklijke Marine | Defensie.nl
Netherlands	Venlo	Hutchison Ports Venlo	None

Source: HutchisonPorts, website.

Table 3: China merchant ports investments in European ports

Countries	Ports	Terminals	Naval bases, NATO and US Armed Forces presence
France	Dunkirk	Terminal des Flandres	None
France	Le Havre	Terminal de France and Terminal Nord	None
France	Montoir	Terminal du Grand Quest	Royal Navy EHI EH-101 Merlin HM1 helicopters at Saint Nazaire Montoir Airport, Loire Atlantique
France	Fos	Eurofos	None
Malta	Marsaxlokk	Malta Freeport Terminal	None
Belgium	Antwerp	Antwerp Gateway	US Armed Forces special agreement for transporting troops NATO in deep water because of Chinese port investments
Greece	Thessaloniki	Thessaloniki Port Authority	None
Netherlands	Rotterdam	Rotterdam World Gateway	Marine Corps | Royal Netherlands Navy; US Armed Forces special agreement for transporting troops NATO in deep water because of Chinese port investments

Source: China Merchant Port, 'We connect the world', Interim report, 2020.

2.3 Risk analysis: from economic dependence to espionage

According to the American Center for Advanced Defense Studies research, Chinese scholars consider investments in maritime dual-use infrastructure necessary for the logistical support of China's long-distance naval operations[41]. The Center referred in its report to a 2015 consensus opinion of Chinese government and university research institutes: 'To accomplish this and defend China's "core interests," these scholars argued that Beijing must cultivate "strategic support states" (战略支点 国家) by building regional cooperation and providing regional public goods for the sake of "making relevant countries believe China's benevolence[42]"'.

In Europe, Member States have in anticipation of, or already existing investment, granted political concessions to China: 'In 2016, Greece, Hungary, Croatia and Slovenia wanted to play down the EU's condemnation of a Permanent Court of Arbitration ruling on China's illegal claim over Philippine territorial waters[43]. In 2017, Greece vetoed the EU's condemnation of China's human rights violations in the United Nations High Rights Council'[44].

Coercion is another tool China is using, applying economic leverage for political aims, such as unofficial sanctions against Japan over territorial disputes in 2010; South Korea over Terminal High Altitude Area Defense systems in 2017; Australia over the inquiry of COVID-19 origin in 2020; and Lithuania over opening Taiwan's representative office in Vilnius in 2022. China's dependencies pose a threat not only in terms of accessing their market but also from imports and infrastructure that facilitates trade for the EU and its Members States with the rest of the world. These dependencies could be exploited for political leverage by rerouting cargo traffic, which in turn affects transit revenues and potentially disrupt the operating system. Such disruptions could lead to the halting or stalling of European consumers' access to critical goods that travel through Chinese-controlled terminals or ports[45].

Based on authoritative Chinese language sources, Isaac B. Kardon and Wendy Leutert argued that China projects power overseas by using a network of commercial ports and dual-use facilities that provide logistics and intelligence support to the Chinese navy[46]. In 2022, Chinese companies owned or operated terminals in 96 ports across 53 countries. It is interesting to underline that the wars in Afghanistan and Iraq brought attention to the trend of military logistics chains becoming increasingly more reliant on the private sector[47]. Kardon and Leutert argued that 'The PLAN has made one or more calls to refuel, resupply, and "show the flag" for diplomacy in at least one-third of PRC companies' overseas ports, … In at least nine ports, PLAN warships have undergone significant repairs or maintenance for vessels and equipment by

[41] D. Thorne and B. Spevack, Harbored Ambitions: How China's Port Investments Are Strategically Reshaping the Indo-Pacific, *C4ADS innovation for peace*, 17 April 2018.

[42] Cited in D. Thorne and B. Spevack, 'Harbored Ambitions', p. 20; Z. Weihua, '习近平时代的中国周边外交：新理念，新概念，新举措"研讨会综述', Seminar Summary of the 'China Periphery Diplomacy of the Xi Jinping Era: New Ideas, New Concepts, New Measures', *China International Studies*, Vol 1, 2015, pp. 135–137.

[43] R. Emmott, 'EU's statement on South China Sea reflects divisions', Reuters, 15 July 2016.

[44] T. Rühlig, B. Jerdén, F.P. Van der Putten, J. Seaman, M. Otero-Iglesias and A. Ekman, Political values in Europe-China relations, report, *European Think-tank Network on China*, December 2018, p. 14; F. Jüris, 'The Talsinki Tunnel: Channelling Chinese Interests into the Baltic Sea', *International Centre for Defence and Security*, 2019.

[45] D. Cristiani, M. Ohlberg, J. Parello-Plesner and A. Small, 'The Security Implications of Chinese Infrastructure Investment in Europe', *The German Marshall Fund, Washington: DC*, 28 September 2021, p. 14; L. Groeneveld and M. Pankowska, 'NATO in deep water because of chinese port investments', *Vsquare*, 18 October 2022.

[46] I. B. Kardon and W. Leutert, Pier Competitor: China's Power Position in Global Ports, *International Security*, Vol 46, No 4, 2022, p. 15.

[47] M. Erbel and C. Kinsey, 'Think again – supplying war: Reappraising military logistics and its centrality to strategy and war', *Journal of Strategic Studies*, Vol 41, No 4, December 2015, pp. 519–544.

making a "technical stop". Two of the nine ports are in Europe'[48]. Mathieu Duchâtel and Alexandre Sheldon-Duplaix state that, 'between 2003 and the end of 2017, PLAN warships have made more than 290 port visits worldwide in all five continents. [...] Naval visits usually reveal zones of influence, prioritised operational zones, intelligence collection objectives and cooperation priorities[49]'.

According to Kardon and Leutert's assessment: 'The PLA almost certainly collects intelligence and conducts surveillance from overseas commercial ports. Although open sources do not detail intelligence operations, terminal operators routinely document valuable and unique information about port facilities and activities'[50]. For instance, during visits, the 'PLA personnel interact with Chinese and local service providers, inspect facilities (including fuel, water, power, and airfield infrastructure), and build local knowledge and relationships'[51].

Long-term high-level security risks related to espionage have been raised about Chinese state-owned enterprise China Logistics Group's acquisition of a 99 years' lease to build a logistics hub in Jade-Weser commercial port close to Germany's biggest navy and logistics base at Heppenser Groden. A German intelligence officer commented on the acquisition: 'Strategic military assets would be advised to turn off their signals when passing, […] There were also tactical risks and the possibility of human intelligence gathering, […]'[52].

Risks of espionage are highest when Chinese commercial assets are located in logistical hubs close to EU and North Atlantic Treaty Organization (NATO) naval bases or port operators hosting Chinese companies, which have signed agreements to provide logistical support to European or American forces. The three largest Chinese shareholders in European ports have assets in almost half the ports (14 out of 29) that are located either close to naval bases or provide logistical support to NATO forces. Compared to Chinese government-owned companies COSCO and China Merchant Ports, the risk level related to the background of shareholders is lower for Hutchison Ports, which is owned by a pro-Beijing tycoon in Hong Kong. With the ongoing erosion of Hong Kong's legal system over time, there is a possibility that the 2017 National Intelligence Law could be applied to Hutchinson in future. This development could potentially increase the risk of espionage from ports in Europe that are operated by Hutchinson.

For example, Hutchinson operates a small terminal (20 ha) in Gdynia, Poland with a lease expiration date in 2104. Hutchinson has shown interest in increasing its presence in Gdynia, which has raised security concerns as Gdynia is an important logistical hub for NATO's eastern flanks' defence against Russia. During the war in Ukraine, Gdynia played a significant role in receiving weapons imports to Ukraine and enabling grain exports from Ukraine[53]. According to Steven Horrell, a former intelligence officer in the US navy: '[…] there are no concerns about a direct war between NATO and China, but rather about China's possible support for Russia. "If you are talking about the Chinese government of the CCP (Chinese Communist Party)

[48] These ports are Alexandria (Egypt), Colombo (Sri Lanka), Dar es Salaam (Tanzania), Port of Djibouti (Djibouti), Piraeus (Greece), Port Klang (Malaysia), Singapore (Singapore), Tanjung Priok (Indonesia) and Valencia (Spain). I. B. Kardon and W. Leutert, Pier Competitor: China's Power Position in Global Ports, *International Security*, Vol 46, No 4, 2022, p. 39.

[49] M. Duchâtel and A. Sheldon-Duplaix, 'Blue China: Navigating the Maritime Silk Road to Europe', European Council on Foreign Relations, 23 April 2018.

[50] 'In routine business, terminal operators observe the callings of ships (including those of foreign navies), their fuel and matériel requirements, the contents of their cargoes, the names of personnel, and their origins and onward destinations. Depending on where dry docks and other facilities are located and how they are utilized, a terminal operator may also observe problems with foreign ships, including their repairs and maintenance. These and other potential observations all provide useful data for both commercial and military intelligence purposes.' I. B. Kardon and W. Leutert, Pier Competitor: China's Power Position in Global Ports, *International Security*, Vol 46, No 4, 2022, pp. 39–40.

[51] I. B. Kardon and W. Leutert, Pier Competitor: China's Power Position in Global Ports, *International Security*, Vol 46, No 4, 2022, pp. 39–40.

[52] D. K. Tatlow, 'China's Stake in World Ports Sharpens Attention on Political Influence', *Newsweek Magazine*, 10 September 2022.

[53] L. Groeneveld and M. Pankowska, 'NATO in deep water because of chinese port investments', *Vsquare*, 18 October 2022.

wanting to support its allies or occasional partner in Moscow. Then yes, there is a lever of influence that could happen through Hutchison"'[54].

2.4 Mitigation: from screening mechanism to implementation

As of February 2023, 18 out of 27 EU Member States have implemented FDI screening mechanisms[55]. Given that ports are crucial transport infrastructures with EU-wide security implications, as exemplified by the case of Gdynia port, it is vital for all Member States to establish their own FDI screening mechanisms to ensure EU security. Besides establishing such mechanisms, it is also necessary to implement them. In 2021, 29 % of all FDIs were subjected to formal screening by Member States, which is higher than the 20 % of cases screened in 2020. However, the percentage of cases rejected in 2021 was lower than in 2020, with only 1 % of cases rejected in 2021 compared to 2 % in 2020[56].

For instance, the port of Hamburg in Germany demonstrates the lack of political will to implement the existing framework for screening foreign investments. Currently, the acquisition of a 24.9 % stake in the Tollerort terminal by COSCO is under revision. Chancellor Olaf Scholz attempted to push through the acquisition despite objections from coalition partners, experts and intelligence services[57]. In hindsight, it appears that there were already legal grounds for objection, as the amount of cargo operated by COSCO qualified the acquisition to be cancelled or limited to a 10 % stake, as with other critical infrastructure cases. Additionally, COSCO failed to apply for the necessary classification of critical infrastructure in a timely manner[58].

To date, Nordic-Baltic countries have shown restraint in regard to China-proposed infrastructure projects, despite half of the region's countries not yet having established FDI screening mechanisms[59]. Among Scandinavian countries that have, there does not appear to be a significant difference from those of their Southern and Western European counterparts[60]. Previous research on connectivity shows the Nordic-Baltic region's cautious stance towards China: 'In the Baltics, it [China] has been interested in Tallinn and Klaipeda ports for over a decade now. In Nordic countries, China has shown interest in Kirkenes and Lysekil ports. In addition, China has been interested in the Talsinki tunnel and Arctic railway projects connecting the Northern Sea Route with the European railway system. In the Nordic-Baltic region, China has so far been unsuccessful in gaining a foothold due to security, feasibility and environmental concerns'[61]. One worry that is not often publicly discussed for frontline countries with Russia is the fear that Chinese companies' control of dual-use strategic infrastructure could hinder US presence or willingness to provide assistance to the region in a conflict scenario with Russia.

National security concerns may not necessarily be shared at subnational level. In 2017, Hong Kong-based Sunbase International, which has close ties to the Chinese government and PLA, was close to building Scandinavia's largest deep-water port (1 800 meters long and 1 000 meters wide dock) in the small Swedish

[54] L. Groeneveld and M. Pankowska, 'NATO in deep water because of chinese port investments', *Vsquare*, 18 October 2022.
[55] European Parliament, List of screening mechanisms notified by Member States, last updated on 2 February 2023.
[56] Report from the Commission to the European Parliament and the Council Second Annual Report on the screening of foreign direct investments into the Union, COM(2022)433, Directorate-General for Trade, 1 September 2022, p. 7.
[57] G. Rinaldi and P. Wilke, Germany rethinks China's Hamburg port deal as further doubts raised, Politico, 19 April 2023; R. Kaljula, 'Europe's Port of Contention', commentary, *International Center for Defense and Security*, 26 October 2022.
[58] G. Rinaldi and P. Wilke, Germany rethinks China's Hamburg port deal as further doubts raised, *Politico*, 19 April 2023
[59] European Commission, List of screening mechanisms notified by Member States, 2 February 2023.
[60] D. Cristiani, M. Ohlberg, J. Parello-Plesner and A. Small, 'The Security Implications of Chinese Infrastructure Investment in Europe', The German Marshall Fund, Washington:DC, 28 September 2021, p. 35; J. Hallberg, 'Foreign investment screening in Finland, Norway, Sweden and Denmark', in S. Hindelang and A. Moberg (eds), *Common European law on investment screening*, Springer, 2021, pp. 209–226.
[61] F. Jüris, 'Chinese Security Interests in the Arctic: From Sea Lanes to Scientific Cooperation', B. Gaens, F. Jüris and K. Raik (eds.), Nordic-Baltic Connectivity with Asia via the Arctic: Assessing Opportunities and Risks, *International Centre for Defence and Security*, 2021, p. 129.

municipality of Lysekil, under the cover of secrecy. The project was only overturned due to the concerns of local citizens and journalists reporting on investors' links with the party-state, despite the project proponent's attempts to downplay their concerns by accusing the other side of alarmism and using the fear of 'missing out' of economic opportunities, which are both standard equipment in the CCP's influence toolbox[62].

3 Beyond direct investment: China's leverage on Europe's rare earth supply

China can gain leverage over EU strategic resources in ways not limited to direct investment. For instance, the rare earth industry, a supplier of resources increasingly critical to the EU's defence and energy capabilities, illustrates the vulnerabilities created by leverage beyond direct ownership. The Chinese government has demonstrated that it is willing to weaponise its overwhelming control of global rare earth supplies to obtain political concessions. The EU's and others' efforts to diversify procurement away from China run counter to China's own policies, which require Chinese control of rare earth resources abroad to preserve its current leverage in the industry. Chinese entities with significant state participation have sought to control some of the world's largest rare earth mines outside China, namely in Greenland and the USA. Even in the absence of direct state ownership links, the party-state enjoys leverage over rare earth projects whose development is critical to Europe's defence and renewable-energy sectors. This section will demonstrate that non-ownership links between China's party-state and critical assets in Europe can lead to vulnerabilities comparable to those created by FDI. At present, while specific vulnerabilities might have been mitigated on an *ad hoc* basis, the EU's regulatory framework does not include tools that could prevent such exposure beyond investment. As Europe's FDI-screening procedures are being consolidated, it can be anticipated that such vulnerabilities created by these loopholes will be increasingly exploited.

3.1 Europe's supply-chain resilience and China's weaponisation of rare earth resources

Rare earth elements, together with other rare metals such as niobium and tantalum, are listed on the EU's Critical Raw Materials List, last revised in 2023. These metals are essential supplies for the defence industry and renewable energy across the world. The EU's climate-neutrality commitments and Member States' responses to risks raised by Russia's invasion of Ukraine contributed to a growing demand in said metals that is expected to continue in the medium term. In 2020, the European Commission estimated that the demand for rare earth elements used in permanent magnets would increase tenfold by 2050[63].

China benefits from an overwhelming control of rare earth mining and processing, an industry which is considered of great strategic importance. Economic security and supporting state capital continue to play key roles under President Xi Jinping. A resolution passed by the 6th Plenum of the 19th Central Committee in 2021 stressed 'self-reliance' as a key concept for the future of China. In this context, priorities in China's economic sector should include 'guaranteeing food safety, energy source security' as well as 'supply-chain security'[64]. In 2016, a plan of the development of the rare earth mining and processing by China's Ministry of Industry and Information Technology stipulates that companies should be supported in 'developing mining for resources abroad' and 'use foreign resources' including overseas talent for the industry's

[62] J. Olsson, 'China's Bid to Build the Largest Port in Scandinavia Raises Security Concerns', *Taiwan Sentinel*, 22 December 2017; C. B. Perlenberg, 'Låt inte Lysekil bli ett nordiskt', *Troja*, Expressen, 20 December 2017.
[63] European Commission, Critical Raw Materials Resilience: Charting a Path towards greater Security and Sustainability, COM(2020) 474 Final, 3 September 2020.
[64] Embassy of the People's Republic of China in Malaysia, '中共中央关于党的百年奋斗重大成就和历史经验的决议（全文）', 16 November 2021.

development and foreign labour for processing. This plan also links rare earth supply safety with 'effectively guaranteeing national strategic resource security'[65].

Adding to its control of rare earth resources, China has repeatedly sought to gain control of major deposits abroad, a strategy consistent with a desire to maintain leverage that China exploited for controversial political ends. Greenland, a constituent country within the Danish kingdom, is home to some of the largest rare earth deposits outside China. In 2016, Shenghe Resources, a Chinese mining company, whose major shareholder is a central government-controlled institute, obtained a stake in Kuannersuit (Kvanefjeld, Greenland) from an Australian licence holder, with the deal including an option for Shenghe to obtain a controlling stake at some point in the future[66]. Mountain Pass, a large rare earth mine in the USA whose reactivation in 2012 threatened to reduce China's control of global supply, saw its US owner forced into bankruptcy due to China's market manipulation which caused a sudden fall in global prices in 2015. The subsequent financial restructuring resulted in the mine's acquisition by a consortium that included Shenghe, the partially state-controlled Chinese miner[67].

Besides China's full supply-chain control, the dominance of the global rare earth market means that the country can opt to take a hostile stance in its achievement of political objectives. For instance, in 2010 the Chinese government imposed export quotas on Japan and cut off exports as it demanded the release of a Chinese captain detained for fishing in waters China claims its own[68]. In 2023, media reports alleged that the government was considering a rare earths export ban[69]. While such drastic measures have not been confirmed, the historical precedent makes an export-restriction scenario possible.

Against the backdrop of China's control versus Europe's scarce domestic mining and processing capacity, the EU is actively seeking to diversify its supplies of strategic raw materials, including rare metals. EU Member States lack active rare earth mines, whilst at the same time significant rare earth mining projects outside of China, such as those in Greenland, have not yet become operational. Furthermore, European processing capacity is also limited, as it is largely concentrated in one facility, namely the **Silmet** plant in Estonia[70]. During the Soviet era, this plant produced enriched uranium, while it currently produces niobium, tantalum and both light or heavy rare earth elements, including cerium, neodymium, praseodymium, samarium, dysprosium, and terbium[71]. In 2021, Silmet announced expansion plans that envisage building a new factory to produce magnets that are used in wind turbines and electric vehicles[72]; this was followed in the following year by Silmet's owner announcing that the company had been awarded a grant of EUR 18.7 million by Estonia's government under the EU's Just Transition Fund for this expansion project[73]. While these plans contribute to Europe's supply diversification efforts, the analysis that follows points to China's indirect leverage over the company in a way that could jeopardise these efforts in the future.

[65] China Ministry of Industry and Information Technology, '稀土行业发展规划（2016-2020年）', 18 October 2016.
[66] M. Martin, 'China in Greenland: Mines, Science, and Nods to Independence', China Brief, Vol 18, No 4, 12 March 2018.
[67] A. Topf, 'Mountain Pass sells for $20.5 million', *Mining.com*, 16 June 2017.
[68] K. Bradsher, 'Amid Tension, China Blocks Vital Exports to Japan', *New York Times*, 22 September 2010.
[69] S. Tabeta, 'China weighs export ban for rare-earth magnet tech', *Nikkei*, 6 April 2023.
[70] Section 3 of the present report includes research separately published in: F. Jüris, 'China and Rare Earths: Risks to Supply Chain Resilience in Europe', *International Centre for Defence and Security*, 31 May 2023.
[71] Neo NPM Silmet, 'About us', webpage, n.d.; J. Sims, 'Letter: This mining facility is not as rare as we thought', *Financial Times*, 28 January 2021.
[72] Eesti Rahvusringhääling, 'Silmet owner to construct €100 million magnet factory in Narva', 9 November 2022; Estonian government, 'Valitsuse pressikonverents, 10. november 2022', Press release, 10 November 2022.
[73] Neo Performance Materials, 'Neo Performance Materials to Receive First-Ever Grant Under Europe's Just Transition Fund for Neo's Planned Sintered Rare Earth Magnet Manufacturing Plant in Estonia', 9 November 2022.

3.2 Neo performance materials' ownership history

Table 4: NPM's ownership history

Names	Years	Ownerships
Magnequech	1986-1995	General Motors.
	1995-2005	Sextant Group.
		San Huan New Material and High Tech.
		China National Nonferrous Metals import and export company.
AMR Technologies	2005	Archibald Cox Jr., Chinese state-owned enterprise.
Neo Material Technologies	2006	Change of company name.
Molycorp	2011	Molycorp acquires Silmet.
Molycorp	2012	Molycorp acquires Neo Material Technologies.
Molycorp	2015	Molycorp files for bankruptcy.
Neo Performance Materials	2016	Oaktree Capital Management.
Neo Performance Materials	2022	Hastings Technology Metals.

Source: author's own compilation, 2023.

3.3 China actors' indirect leverage on Europe's rare earth processing

The sole rare metal processing plant in Europe is owned by a Canadian company whilst its largest corporate shareholder is an Australian rare earths developer. Although there is no direct control by China, the companies involved in the plant have connections that could potentially provide China with significant leverage. Upon analysing these companies, it becomes evident that the Chinese government and state-owned companies have a continued interest in them. Some of these companies' predecessors were partially owned by Chinese state-owned companies, received subsidies from Chinese state agencies and had assets that Chinese state interests sought to acquire.

The Silmet plant is currently controlled by Canadian-based **Neo Performance Materials** (NPM), through an Estonian subsidiary. NPM emerged in 2016 from the restructuring of Molycorp, which once owned the USA's largest, rare earth mine[74]. In 2022, Hastings Technology Metals Ltd, an Australian rare earths developer, was the largest shareholder of NPM[75]. Although Silmet is not currently controlled by Chinese interests, NPM and its predecessors have a history of Chinese ownership that goes back to China's former leader, Deng Xiaoping, and his efforts to develop China into a rare earths power. What is now NPM's magnet-producing arm, **Magnequench**, was acquired from General Motors in 1995 by a consortium of two Chinese state-owned enterprises, as the Chinese government plan sought to develop the rare earths

[74] Milbank, 'Milbank Represents Oaktree Capital Management in Successful Reorganization of Molycorp, Inc.', 1 April 2016 [web archive].
[75] Wyloo Metals, 'Wyloo Metals Invests $150 Million In Rare Earth Materials', 26 August 2022 [web archive]; Mining Technology, 'Hastings acquires stake in Neo Performance Materials for $97m', 14 October 2022; P. Ker and B. Thompson, 'Forrest pumps $150m into rare earths aspirant', *The Australian Financial Review*, 26 August 2022; A. Macdonald, S. Thompson and K. Sood, 'Hastings Tech Metals readies $100m-odd raise after Wyloo investment', *The Australian Financial Review*, 5 September 2022.

sector[76]. By 2001, Magnequench production facilities had relocated to China. However, successive mergers and acquisitions gradually diluted Chinese ownership of NPM's predecessor entities through the 2000s, until Molycorp the then-owner of the USA's Mountain Pass rare earths mine acquired it in 2012[77]. Thereafter, Molycorp's bankruptcy and subsequent restructuring brought Chinese interests back to entities controlling Silmet. Oaktree Capital Management, a US-based company, which became NPM's largest shareholder, had previously received an investment of USD 1 billion from a Chinese state-owned investment fund[78]. In August 2022, the Australian mining and metals business Wyloo Metals, ultimately owned by mining magnate Andrew Forrest's family, announced a 150 million Australian dollar investment in Hastings, for the latter to acquire a 22.1 % stake in NPM from Oaktree[79].

The links of NPM and its predecessors to China indicate a pattern of interest and leverage by the Chinese government and state-owned companies. The collapse of NPM's direct predecessor, Molycorp, itself followed a drop in rare earth element prices caused by China's fluctuating market controls[80]. Molycorp's flagship asset, the Mountain Pass mine, key to the West's supply-chain resilience, was then sold to a consortium that included Shenghe Resources, the partially state-controlled company that also sought to control Greenland's largest, rare earth mine[81]. In 2013, Oaktree, until recently NPM's largest shareholder, established a joint venture with Cinda (中国信达), a Chinese state-owned asset management company, to 'jointly invest in distressed assets in China and to cooperate with respect to distressed assets investments in markets outside China' – a goal arguably consistent with Oaktree's role in the Molycorp restructuring three years later[82].

This pattern of leverage is ongoing. NPM's operations in China still account for a significant part of its revenue. Wyloo Metals, owned by the investment fund Tattarang, provided funding to Hastings for the acquisition of NPM. Tattarang is still owned by the family of the Australian mining entrepreneur Andrew Forrest, whose links with China are particularly extensive. His main business, **Fortescue Metals Group**, mines and exports iron ore to China, which is the company's primary market for this product. Forrest has been repeatedly linked to China's party-state's attempts to influence his home country's politics. Australian media investigations noted that one of Forrest's China contacts in the 2010s was a leading figure within the China Association for International Friendly Contact, a political influence platform run by one of the PLA's intelligence agencies[83]. These contacts were followed by Forrest's businesses organising Australian

[76] J. Tkacik, 'Magnequench: CFIUS and China's Thirst for U.S. Defense Technology', Heritage Foundation, 2 May 2008; *South China Morning Post*, 'Onfem in US magnetic', 7 January 1997 [web archive]; Liaowang Institute, '中国的稀土有多重要？', 21 May 2019 [web archive]; Caijing, '中国钕铁硼出口遭日本专利壁垒', 14 July 2014 [web archive]; Association of China Rare Earth Industry, '日立金属专利被判无效 稀土产业联盟告捷', 25 February 2016 [web archive].

[77] Reuters, 'Molycorp buys Neo Material for C$1.3 billion', 9 March 2012.

[78] *Shanghai Securities Journal* via Economic Daily, '中投将向橡树资本投资10亿美元 双方都保持低调', 28 September 2009 [web archive]; *China Times*, '中投：千亿资金转向能源资源领域', 07 December 2009 [web archive].

[79] Wyloo Metals, 'Wyloo Metals Invests $150 Million In Rare Earth Materials', 26 August 2022 [web archive]; Mining Technology, 'Hastings acquires stake in Neo Performance Materials for $97m', 14 October 2022; P. Ker and B. Thompson, 'Forrest pumps $150m into rare earths aspirant', *The Australian Financial Review*, 26 August 2022; A. Macdonald, S. Thompson and K. Sood, 'Hastings Tech Metals readies $100m-odd raise after Wyloo investment', *The Australian Financial Review*, 5 September 2022.

[80] *Mining Engineering*, 'Molycorp completes work on its Phoenix Project, names new CEO', 9 October 2013 [web archive].

[81] A. Topf, 'Mountain Pass sells for $20.5 million', *Mining.com*, 16 June 2017.

[82] Oaktree Capital Group, 'Oaktree and China Cinda Asset Management Announce Joint Venture', 25 November 2013 [web archive]; Caixin, '信达与橡树资本共同投资中国不良资产', 26 November 2013 [web archive].

[83] The agency, then known as the PLA General Political Department's Liaison Department, has since become the PLA Political Work Department's Liaison Bureau. See, J. Garnaut, 'Australia's China reset', *The Monthly*, August 2018; J. Garnaut, 'Chinese military woos big business', Sydney Morning Herald, 25 May 2013; M. Stokes and R. Hsiao, 'The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics', Project 2049, 14 October 2013, p. 20; G. Wade, 'Spying beyond the façade', *Australian Strategic Policy Institute*, 13 November 2013; China Association or International Friendly Contact, 'Honorary Chairman Xu Kuangdi Meets with the Business Leaders from Australia', 29 July 2012; China Association or International Friendly Contact, 'Vice-chairman Deng Rong Meets with Guests from Australia', 9 April 2013.

participation in exchanges surrounding the Bo'ao Forum, an international platform organised by China that promotes the party-state's views[84]. During the COVID-19 pandemic, Forrest appeared to espouse views on the virus' origin aligned with China propaganda, arguing that 'it just might be Australia, it just might be Britain' in remarks that earned a direct condemnation from the country's prime minister[85].

Silmet's owner may also have indirect ties to China's defence sector that warrant further investigation. The Singapore-based research and development centre of NPM subsidiary Magnequench is led by Chen Zhongmin. Zhongmin was educated at Northwestern Polytechnical University and previously worked for a subsidiary of the Aviation Industry Corporation of China[86], a key supplier to both civilian and military aerospace industries which has been sanctioned by the USA and Japan[87]. Northwestern Polytechnical University is one of the 'seven sons of national defence', a group of Chinese civilian universities subordinated to the Ministry of Industry and Information Technology, a key component of China's defence sector[88].

The potential for connections to high-risk actors to go undetected was highlighted in 2022 by an NPM-linked company in Estonia when NPM and local partners set up a joint venture, **MQ HPMG Europe**. The company's name combined the acronyms of both NPM's magnet-producing wing Magnequench and a Chinese market leader in the same field, Hangzhou Permanent Magnet Group (HPMG, 杭州永磁集团有限公司)[89]. In the first quarter of 2019, HPMG was one of the five largest suppliers to Xi'an Tianhe Defense Technology (西安天和防务技术), a private defence company that has provided services to the Chinese military for 19 years and has obtained various military industry credentials in domains including radar detection, photoelectric detection and underwater acoustic detection[90]. According to a Silmet managing director and board member, the name was chosen by lawyers assisting NPM, who was at the time negotiating patent and technology acquisitions with HPMG. Those negotiations were ultimately unsuccessful[91]. In November 2022, MQ HPMG Europe renamed **Magnet Ventures Europe** and later **NPM Narva** in March 2023, with the Executive Vice President of Magnequench becoming one of its directors[92]. Although no active link between HPMG and Silmet is known, this incident showed how without the necessary government scrutiny business contacts in a China-dominated industry could lead to Chinese defence sector actors becoming involved in EU strategic projects.

[84] Fortescue, 'Fortescue to be Diamond Partner of the 2020 Boao Forum for Asia', News, 16 January 2020 [web archive]; Fortescue, '与中国的合作', webpage, n.d. [web archive]; Fortescue, 'Fortescue Metals Group steps up as a strategic partner of the 2021 Boao Forum for Asia', News, 21 April 2021 [web archive].

[85] M. Robin, 'Where did COVID-19 come from? Don't ask Twiggy Forrest', The Australian Financial Review, 3 April 2020; S. Maiden, 'Scott Morrison hits out at suggestion by Andrew 'Twiggy' Forrest COVID-19 could have originated in Australia', News.com.au, 1 May 2020.

[86] Neo Magnequench '研究与创新', webpage, n.d. [web archive]; See the public LinkedIn profile of Zhongmin Chen, R&D Manager at NEO Magnequench; Cn.TTFLY, '中航工业西安航空发动机集团有限公司', webpage, n.d [web archive]..

[87] China Defence Universities Tracker, 'Aviation Industry Corporation of China', last updated on 18 November 2019.

[88] China Defence Universities Tracker, 'Northwestern Polytechnical University', last updated on 6 May 2017.

[89] Estonian e-business Register, 'MQ HPMG Europe OÜ (16493223)', webpage [web archive].

[90] Money Finance Sina, '天和防务：2019年第一季度报告全文', 26 April 2019 [web archive]; Tianhe Defens, '公司简介' webpage, n.d. [web archive]; Tianyancha, '西安天和防务技术股份有限公司', webpage, 2022 [web archive]; Baidu Aiqicha, '西安天和防务技术股份有限公司', webpage, n.d.

[91] Raivo Vasnu, email correspondence with the author, 4 May 2023.

[92] Estonian e-business Register, 'MNP Narva OÜ (16493223)' (or Magnet Ventures Europe) webpage, n.d.; Search for 'Magnet Ventures Pte. Ltd' through the Acra register for entities and public accountant. Business Filing Portal Of ACRA, webpage, n.d. ; Neo Performance Materials, 'Who we are' webpage, n.d. [web archive]; See the public LinkedIn profile of Shan Zhan 单湛, Vice Presidence of Sales and Marketing at Magnequench.

3.4 Europe's vulnerability to China's weaponisation of non-ownership leverage

Given the existing ownership structure of the Silmet plant, there is no immediate risk that the Chinese government will take control of EU's rare earth supply chain and its allies in the immediate future. However, the fact that Silmet is exposed to the Chinese market makes the efforts to enhance European supply-chain resilience vulnerable to China's actions, which contradict EU policy goals. This means that China's ability to exert pressure on actors within the Chinese market could undermine the EU's efforts to strengthen and make its supply chain more resilient.

China has repeatedly weaponised its control of global rare earth mining and processing. The CCP's current economic and foreign policy indicates such measures will continue, becoming increasingly hostile regarding the EU's efforts to build supply-chain resilience in this strategic resource. Thus, it appears likely that future China-led measures will use their leverage on Western rare earth producers to hamper European capacity building. While the Canadian company behind Silmet has become a participant in these EU efforts, the prominent Australian businessperson associated with its largest shareholder has repeatedly appeared to be aligned with CCP's influence and propaganda operations. Given the company's reliance on its China operations and the precedent of Chinese government involvement in similar cases, it is possible that the Chinese government could use regulatory and informal measures to influence Silmet's business decisions, potentially jeopardising one of the company's main revenue streams.

If the Chinese government were to use its leverage over the owner of a European strategic rare earths asset to coerce it into following China's policies, the production of key strategic resources could quickly fall below the needs of Europe's defence and other industries. In this strategic sector, a company's dependence on the Chinese market and a history of susceptibility to CCP influence can pose a risk similar to that posed by China's ownership stake.

3.5 Mitigating non-investment vulnerabilities

While there is nothing to indicate that proper due diligence did not take place before awarding the Silmet plant's owner a role in European supply-chain resilience-building projects or regulatory approvals in Estonia, such procedures do not appear to be mandated by current EU or Member State regulatory frameworks. In the absence of direct investment by Chinese entities, EU strategic assets can be bought and sold without necessarily triggering a mandatory analysis of China's non-ownership leverage on the asset's controlling entity. Any vulnerabilities currently created by Chinese leverage (among other vulnerabilities) could be mitigated by requiring asset owners to reduce their China-market exposure through disinvestment. However, the current regulatory framework has not created tools that could justify or enforce such a requirement.

Avoiding all cooperation with companies linked to China might prove impossible in a sector overwhelmingly dominated by China. However, investment screening, grant and subsidy awards together with other regulatory processes could reduce China's influence on businesses involved in critical infrastructure by making finer distinctions between degrees of connection to China. Additional demands could be put on investors or grant awardees, incentivising a gradual delinking from the China party-state influence networks. Furthermore, EU stimulus to the rare earths industry, such as the development of additional mining and processing capacity, coupled with stronger scrutiny of China's leverage on the businesses involved, could diversify the sector, and reduce exposure to individual channels of China's influence.

4 A Chinese company in the backbone of Europe's internet infrastructure

The Chinese company **HMN Technologies** has constructed and upgraded undersea data cable systems connecting EU Member States' territories and the Indo-Pacific region that hosts military bases belonging to Member States and NATO. This development could potentially allow China to collect intelligence from these countries and share it with Russia, as well as potentially other adversarial countries. Additionally, the owner of HMN Technologies, Hengtong Group, is involved in building underwater surveillance systems in the South and East China seas. If undersea cable systems based on HMN technology are located near naval ports belonging to Member States and NATO, they could be used for underwater surveillance, which would compromise EU and NATO security.

4.1 Background: digitalisation demands better cyber security

By early 2023, there were around 552 active or planned cable systems with a total length of 1.4 million km[93]. Undersea cables laid on the ocean floors enable the transfer of nearly all trans-oceanic data comprising internet, phone calls and TV broadcasts[94]. In an increasingly interconnected world that depends heavily on digital services the demand for data bandwidth is likely to increase even further. Between 2019 and 2021, the amount of internet bandwidth used by global networks almost doubled, reaching 2900 terabits per second. Similarly, between 2018 and 2020, it also doubled and reached 2000 terabits per second[95]. In the EU, Member States have reached high levels of digitalisation, with the vast majority (94.2 %) of EU enterprises having fixed broadband connection by 2022 and 50 % of the EU enterprises holding meetings using online platforms. During 2021, at least one in every five EU companies was conducting e-sales[96]. These numbers are likely to increase over time as the Internet of Things is implemented.

In December 2022, the European Council approved the CER Directive, where critical infrastructure is defined as: '…an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service.' The same Directive defines an essential service as: '…service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment'[97]. In digitalised societies such as those that form the EU, all 11 sectors of critical infrastructure from energy to space, as defined in the directive, depend on a stable internet connection[98]. The current NIS2 Directive adopted in January 2023 does not provide concrete measures for Member States regarding risk mitigation, but generally stipulates that 'Member States should ensure that the security of the public electronic communications networks is maintained and that their vital security interests are protected from sabotage and espionage'. However, this Directive does suggest that 'The national cybersecurity strategy should, where relevant, take into

[93] TeleGeograph, 'Submarine Cable Frequently Asked Questions', webpage.
[94] N. Starosielski, *The Undersea Network: against the flow*, Duke University Press, 2015.
[95] P. Brodsky, 'Content Providers Binge on Global Bandwidth ', TeleGeography Blog, 22 June 2022.
[96] Eurostat, 'Use of digital technologies among EU enterprises', 20 January 2022.
[97] See Article 2. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)', Official Journal of the European Union, L 333/164, 27 December 2022.
[98] Critical sectors of infrastructure: energy, transport, banking, financial market infrastructure, digital infrastructure, drinking and waste water, food (including production, processing and delivery), health, public administration and space infrastructure; European Parliament, 'MEPs approve new rules to protect essential infrastructure', Press Release, 22 November 2022.

account the cybersecurity of undersea communications cables and include a mapping of potential cybersecurity risks and mitigation measures to secure the highest level of their protection'[99].

Undersea cables are also important for the defence and security of EU Members States. 'In the age of digital warfare and integrated platforms, most EU Member States' defence capabilities are connected digitally. This relates to command-and-control structures, but also integrated weapon systems, including drones and aircraft carriers[100]. In 2017, a Dutch company sold the backbone of Estonia's internet infrastructure, which included undersea cables connecting Estonia with EU and NATO Member States (the Netherlands, Finland and Sweden) as well as the Tallinn Exchange Point, to a Chinese company with links to the PLA, without any public discussion. This sale has raised serious concerns not only about Estonia's security, but also that of the EU and NATO, as Tallinn is home to both the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA) and the NATO Cooperative Cyber Defence Centre of Excellence[101]. In 2019, 75 % of the Estonian Defence Forces' external communication was contracted to go through the same infrastructure controlled by the above-mentioned Chinese company. The Estonian cyber security authorities stated that the risks of espionage posed by China's 2017 National Intelligence Law, which obligates companies to cooperate with intelligence services, were mitigated by using data encryption[102].

In recent years, there has also been an increasing concern about attacks on undersea cables, especially when it concerns cables using dual-use technology such as satellite ground stations or underwater surveillance systems. According to Daniel S. Hamilton and Joseph P. Quinlan, 'In November 2021, a network of undersea sensors belonging to the Norwegian Ocean Observatory was cut; two months later, the undersea cables connecting Norway's Svalbard Satellite Station to the mainland were cut. Impaired operations at that station, which connects to Europe's Galileo satellite system, could cripple the EU's ability to monitor maritime infrastructure'[103].

In October 2022, before the adoption of the CER Directive, a draft recommendation called for increased cooperation with key partners, neighbouring countries and NATO. At that time, the Vice-President for Promoting our European Way of Life, Margaritis Schinas, stated that 'Critical infrastructures have become increasingly interlinked as well as mutually dependent. Be it pipelines, transport ways, or undersea cables, a disruption in one country can have a cascading effect with ramifications for the Union as a whole. The Commission acted early on in our mandate to build a robust system to protect infrastructure online and off. The Nord Stream sabotage and other recent incidents show we need to accelerate the implementation of this new system and build strong crisis coordination mechanisms to act today.'[104]

It is worth noting that the most common threat to undersea cables is unintentional human activity such as fishing, where boats accidentally damage cables on the sea floor which are no wider than garden hoses. These risks are mitigated by spreading capacity over multiple cables to be able to reroute traffic when needed.

[99] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), Official Journal of the European Union, L333/80, 27 December 2022.
[100] C. Bueger, T. Liebetrau and J. Franken, 'Security threats to undersea communications cables and infrastructure – consequences for the EU', Policy Department for External Relations, PE 792.557, June 2022, p.16.
[101] F. Jüris, 'Estonia's Evolving Threat Perception of China', *The Prospect Foundation*, Prospects & Perspectives, No 25, 26 April 2022.
[102] H. Roonemaa, M. Eesmaa, I. Liepina, S. Bērzina and N. Navakas, 'Hiina luure võtab Eesti üha jõulisemalt sihikule', *Postimees*, 5 September 2019.
[103] D. Hamilton and J. Quinlan, 'Chapter 5: The Digital Drivers of the Transatlantic Economy' in The Transatlantic Economy 2023: Annual Survey of Jobs, Trade and Investment between the United States and Europe, Washington, DC: Foreign Policy Institute, Johns Hopkins University, p. 77.
[104] European Commission, 'Critical Infrastructure: Commission accelerates work to build up European resilience', Press Release, IP/22/6238, 18 October 2022.

4.2 Undersea communication cables close to military bases

Table 5: Undersea communication cables

Name	Supplier/ Upgrader	Military base	Year	Landing Point
Avassa	HMN	Navy Base in Mayotte	2016	Mamoudzou, Mayotte
Flores-Corvo Cable System	HMN	Naval Air Station Lajes Portugese and US Air Force	2014	Azores, Portugal
HANNIBAL System	HMN	Naval Air Station Sigonella	2009	Mazara del Vallo, Italy
PEACE Cable	HMN	Akrotiri, Episkopi, Dhekelia and Ayios Nikolaos (UK Sovereign Base Areas)	2022	Yeroskipos, Cyprus
		ORION Maritime Patrol and Reconnaissance Aircraft Detachment (EU Naval Force Operation ATALANTA)	NA	Djibouti City, Djibouti
		Istres-Le Tubé Air Base	NA	Marseille, France
		Armed Forces of Malta (Hay Wharf Base in Floriana, Mgarr Harbour and Qortin Base in Gozo)	NA	Mellieha, Malta
Silphium	HMN	Crete Naval Base (Hellenic Navy); NSA Souda Bay (NATO)	2013	Chania, Greece
West Africa Cable System	Alcatel Submarine Networks/HMN	STRIKFORNATO - Naval Striking and Support Forces NATO	2012	Oieras and Seixal, Portugal
		Joint Analysis and Lessons Learned Centre, or the JALLC	NA	Seixal, Portugal
		Las Palmas Naval Base	NA	El Goro, Canary Islands, Spain
C-Lion1	ASN/HMN	Upinniemi Garrison	2016	Helsinki, Finland
		Warnemünde Naval Base Command	NA	Rostock, Germany
Greenland Connect	ASN/HMN	Thule Military BASE	2009	Greenland
MedNautilus Submarine System	ASN/HMN	Naval Support Activity Souda Bay	2001	Pentaskhinos, Cyprus
		Akrotiri, Episkopi, Dhekelia and Ayios Nikolaos (UK Sovereign Base Areas)		Athens, Greece
		Naval Air Station Sigonella		Catania, Italy
Pencan 8	ASN/HMN	Las Palmas Naval Base	2011	Canary Islands, Spain
Pencan 9	HMN	Las Palmas Naval Base	2016	Canary Islands, Spain

Source: author's own compilation, 2023.

4.3 China's cable system providers ties with the party-state and PLA

The Chinese company HMN Technologies has a significant share in the global undersea cables market and between 2009 to 2022 built or upgraded 11 systems for European internet users. HMN's majority shareholder is Hengtong Group, whose controlling shareholder is a former decorated PLA veteran, CCP member and delegates at the 12th and 13th National People's Congress. The Hengtong Group of companies has been involved in China's national underwater surveillance systems projects in the East and South China seas and its representatives have expressed intent to build such systems for both military and civilian use at strategic locations all around the world. Hengtong is a member of the industrial MCF alliance and has established a joint venture and research lab with a PLA-intelligence-related entity, whose other branches have been accused of industrial espionage.

According to a Submarine Telecoms Forum report, Chinese undersea cable system supplier HMN Technologies was, between 2018 and 2022, the second biggest supplier with 15 systems after Finnish Alcatel Submarine Networks (ASN) with 27 systems and ahead of American SubCom with 15 systems globally. For the same period, HMN together with SubCom held third place with 16 % of systems installed after French Orange at 17 % and ASN at 28 %. For the period 2018 to 2022, SubCom took the lead on total systems length with 118 000 km of cable, followed by ASN's 88 800 km and HMN's 55 700 km[105]. Based on a dataset compiled from the websites of HMN and the telecommunications market research company TeleGeography, between 2009 and 2022, HMN constructed or updated 11 undersea cable systems connecting territories of EU Member States and the Indo-Pacific.

HMN was formerly known as Huawei Marine Networks, a subsidiary of Huawei Technologies. According to one of their press releases, 'In the first half of 2020, Hengtong group completed the 81 % shareholding acquisition of Huawei Marine Networks Co., Ltd. New Saxon 2019 Ltd. (UK) holds the remaining 19 % balance of shares'[106]. In June 2022, New Saxon was bought from HMN and Hengtong's shares through subsidiaries increased to 93 %, while the remaining 7 % were acquired by Suzhou Qiyuan Equity Investment Management Partnership (Limited Partnership) (苏州华智创业投资合伙企业)[107].

The Hengtong Group's majority shareholder with 90 % of the shares is Genliang Cui (崔根良)[108]. Cui, who has been involved in the communication cables business since 1991, served as a PLA Airforce communication specialist in his youth and became a member of the CCP during his military service. He has also served as a member of the 12th and 13th National People's Congress. Furthermore, in 2019, Cui was awarded the title of 'National Model Veteran' and in 2021 he received the award of 'National Outstanding Communist Party Member'. Under Cui's leadership, Hengtong has pursued an internationalisation strategy since 2010, becoming part of the BRI framework in 2013[109].

In June 2017, China's central government approved the construction of the Underwater Science Observation Network (海底科学观测网) in the South and East China seas with an estimated cost of CNY 2.1 billion (EUR 2.8 billion). This project was led by Tongji University and was supposed to be finished in five years. The Observation Network was required to provide real-time 3D monitoring of the ecosystem[110]. Construction of the project began in 2019, with an estimated completion date of 2024. However, by August 2020 physical construction of the monitoring and data centre in Shanghai had already been completed[111].

A few months before the announcement, Tongji University and the Hengtong Group established a joint venture called Shanghai Hengtong Marine Equipment to integrate Tongji University's scientific and Hengtong's industrial expertise in underwater surveillance[112]. With the establishment of this joint venture,

[105] Submarine Telecoms Forum, 'Submarine Telecoms Industry Report 2022-2023', Vol 11, 2022, pp. 56-58.
[106] HMN Technologies, 'Huawei Marine Networks Rebrands as HMN Technologies', Press release, 3 November 2022 [web archive].
[107] Hengtong Group, webpage, 21 February 2023 [web archive]; Asset Management Association of China, '私募基金管理人公示信息', Information annoucement, 8 April 2023 [web archive]; Qiming Venture Partners, webpage, 9 december 2022 [web archive].
[108] Baidu, webpage, 8 April 2023 [web archive].
[109] Hengtong Group, '小"通道"走出大人生——记亨通集团党委书记、董事局主席崔根良' webpage, 27 December 2020; Hengtong Group, '亨通集团董事局主席 崔根良', webpage, 1 October 2022.
[110] Gov.cn, 我国将建设国家海底科学观测网', webpage, 6 August 2017.
[111] Mlab Tongji, '国家海底科学观测网', webpage, n.d [web archive]; The Paper, '国家海底科学观测网建设进展：监测与数据中心主体结构封顶', webpage, 9 March 2020 [web archive]; People.cn, '为建设海洋强国贡献深蓝科技力量（科技名家笔谈）', webpage, 14 April 2022 [web archive].
[112] Academy of Ocean of China, '建设海底观测网迫在眉睫', webpage, 17 January 2019 [web archive].

the Group hoped to take the lead in developing underwater surveillance systems for both civilian and military use[113].

In 2017, Sun Guilin (孙贵林), deputy general manager of Shanghai Hengtong Marine Equipment, who has been involved with the national ocean observation network project, revealed that in future the Observation Network will cover not only China's coastal areas, distant and regional waters, but also important points in international waters and polar regions[114].

Jiangsu Hengtong Ocean Optical Network System from the Hengtong Group is a member of the Z-Park Joint Innovation Civil-Military Integration Equipment Industry Alliance Enterprise Service Platform (中关村联创军民融合装备产业联盟) in Beijing. According to the alliance's website, it was established in 2014 and is the first industrial alliance to include the MCF framework as its key function[115]. In September 2017, at the '3rd Military-civilian Integration Development High-tech Equipment Achievement Exhibition' (第三届军民融合发展高技术装备成果展), Hengtong's Submarine Observation Network received praise from leaders of the Central Military Commission (the Ministry of National Defence) for its private sector contribution to national defence[116].

In 2018, Jiangsu Hengtong Optic Electric established a joint venture and research laboratory for industrial control system information security with the Jiangsu Province branch of the National Information Security Engineering Technology Center (NISEC)[117]. Such systems are computer systems that monitor and control industrial processes and infrastructure[118]. A Press release from the signing of a cooperation agreement for the joint laboratory stated that 'The industrial control system is the "nerve centre" of the national industry, which is related to the economic security, political security and social stability of the country'[119].

According to PLA experts L.C Russell Hsiao and Mark A. Stokes, the PLA General Department Third Department, the likely leading authority of cyber surveillance, maintains administrative oversight of NISEC and its bases in Shanghai, Beijing and Tianjin, which the authors believe to be involved in: '[…] training a new generation of cyber operations specialists; national information security bases appear to function as clusters that leverage academic and entrepreneurial talents of host cities'[120]. Media reporting based on co-authorship of cybersecurity-related papers and the analysis of China cyber experts' CVs has confirmed some of these claims, where NISEC and its bases are affiliated with PLA Unit 61398, which has been accused of industrial espionage[121]. Further investigation is needed to confirm a similar overlap by this Jiangsu base

[113] Hengtong Group, '国家海底科学观测网正式获批 亨通提前布局占据行业先机', webpage, 6 January 2017 [web archive].
[114] Hengtong Group, '科技日报：深海观测网： 给海底来个360度扫描', webpage, 7 July 2017 [web archive].
[115] Z-Park Joint Innovation Civil-Military Integration Equipment Industry Aliance Enterprise Service Platform, '江苏亨通海洋光网系统有限公司', webpage [web archive] and '联盟简介', webpage [web archive].
[116] News.bjx.com.cn, ' 亨通海底观测网受中央军委、国防部等领导关注与好评', 25 September 2017; Cshtgw.com, '亨通海底观测网受中央军委、国防部等领导关注与好评', Hengton Port, webpage, 3 January 2018.
[117] Hengtong Group,'江苏亨通信息安全技术有限公司', webpage, n.d [web archive]; Aiquicha Baidu, '江苏亨通工控安全研究院有限公司', webpage, n.d [web archive]; Sohu, ' 重磅 | 亨通成立未来工控系统信息安全国家级联合实验室 ', 6 July 2017 [web archive].
[118] C. Neagu, 'Industrial Control System (ICS): Definition, Types, Security', Heimdal, 8 February 2023.
[119] Hengtong Group, '亨通成立未来工控系统信息安全国家级联合实验室', 7 May 2018; Sohu, ' 重磅 | 亨通成立未来工控系统信息安全国家级联合实验室 ', 6 July 2017.
[120] M. A. Stokes and R. Hsiao, 'Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests', *Project 2049 Institute*, 29 October 2012; National Information Security Engineering Center, webpage, n.d.
[121] M. Lee, 'Top China college in focus with ties to army's cyber-spying unit', *Reuters*, 24 March 2013; Z. Doffman, 'Huawei Employees Linked To China's Military And Intelligence, Reports Claim', *Forbes*, 6 July 2019.

with the structure and role of the PLA General Department Third Department after the 2017 reform, where it became part of the PLA Strategic Support Force as The Network System Department[122].

4.4 Risks analysis: from espionage to underwater surveillance

There has been increased awareness about cybersecurity risks posed by China in the EU regarding ICTs, which have led to concrete actions by EU Member States, referred to earlier, in banning Huawei products from their mobile networks to limiting usage of the Chinese social media app TikTok in government devices. Undersea cables that make up the backbone of internet infrastructure have received little or no attention regarding potential threats posed by China. This is disproportional to its importance to the functioning of almost all critical infrastructure in a digitalised society.

HMN Technologies controlling shareholder Hengtong's joint venture and research lab with PLA cyber intelligence affiliated entity increases the risk of espionage and improves China's access to sensitive information as both diplomatic and military communication travels through privately-owned undersea cables provided by Chinese companies. According to the 2017 National intelligence law, all Chinese entities are obliged to cooperate with the country's intelligence services. Taking into consideration that HMN provided undersea cables at strategic locations close to EU Member States and NATO military bases, based on the Estonian Defence Forces example, it cannot be ruled out that these cables are used for communication between allies and maybe even for operating complex military systems such as drones[123].

Distributed Acoustic Sensing technology facilitates the turning of undersea fibre optic cables into underwater sensors without hampering data transfer capabilities[124]. HMN's parent company's joint venture for building underwater surveillance systems and involvement in China's national underwater surveillance system project makes it highly likely that HMN possesses the necessary expertise to turn its existing underwater cables into underwater surveillance systems. HMN-laid cables at strategic locations close to the EU and NATO Member States' naval bases and strategic passages enable the CCP to monitor the movement of EU and NATO Member States' naval vessels. This is a high-level security vulnerability when it comes to China's capability to detect and monitor the movement of ballistic missile submarines thereby hampering the nuclear deterrence capabilities of the USA and its allies. Russia has used nuclear threats in the context of its war in Ukraine. Moreover, this cannot be ruled out in Taiwan's contingency scenario.

The 'Sino-Russia' 'limitless' partnership *does* have certain limits such as large-scale military assistance to Russia's war in Ukraine still on hold for the moment. Nevertheless, great interest has been established in strategic projects from plans for a joint Moon station to Russia's assistance in building an early warning system for China to a high-level institutionalised Arctic underwater acoustics cooperation with potential significance for both countries' nuclear deterrence capabilities[125]. By comparison, if the USA shares intelligence with its allies, it is possible that China could also share intelligence collected using undersea cables with its strategic partner.

4.5 Mitigation: from FDI screening to scrutiny of the suppliers

EU Member States' current awareness and risk mitigation frameworks overlook security risks coming from the suppliers of undersea cable systems because they focus mainly on the need to protect undersea cables

[122] T. Wu and C-L Hung, 'Chapter 8 Cyber Warfare Capabilities of the PLA Strategic Support Force (SSF)', *Institute for National Defense and Security Research*, 2022, p. 100.
[123] C. Wall and P. Morcos, 'Invisible and Vital: Undersea Cables and Transatlantic Security', *Center for Strategic and International Studies*, 11 June 2021.
[124] F. Jüris, 'Handing over infrastructure for China's strategic objectives: 'Arctic Connect' and the Digital Silk Road in the Arctic', *Sinopsis*, 7 March 2020.
[125] F. Jüris, 'Sino-Russian Scientific Cooperation in the Arctic: From Deep Sea to Deep Space', in S. Kirchberger, S. Sinjen and N. Wörmer (eds), *Russia-China Relations: Emerging Alliance or Eternal Rivals?,* Springer, 2022, p. 185-202.

from outside intrusions or malign attacks. For example, Ireland proposed to enhance sub-surface capabilities for monitoring undersea cable systems[126]. Portugal, sharing Ireland's mostly Russia-related concerns, has proposed considering this topic in the Strategic Compass and the EU Maritime Security Strategy[127].

According to France's Ministry of the Armed Forces, the 2021 French Seabed Strategy domestic law is being revised thereby requiring operators to provide prior notice of the cable routes laid in France's Exclusive Economic Zone and continental shelf. In addition, a legal framework for preliminary studies and system authorisation is being contemplated[128]. In France, regular checks and detection of damage to cables fall under the responsibility of cable-supplying companies[129]. In Denmark, cable owners and operators are responsible for the surveillance and protection of undersea cables and are required to install monitoring and surveillance systems for that purpose[130].

In HMN Technologies' case, where a Chinese company is obliged by law to grant Chinese intelligence services access to its governed data, there is no actual need to fear outside intrusion or military attack on the cables systems, which makes it unnecessary to mitigate the security risk by enhancing naval capabilities similarly to Ireland. Neither could outside monitoring prevent a Chinese cable system supplier from sharing data with its intelligence services. Even though there is to date no publicly available information regarding evidence of intelligence-sharing taking place between China and Russia, this could nevertheless already be happening or at least being progressed as the 'Sino-Russian strategic partnership' continues to grow. An additional worry is Chinese suppliers' potential to build bugs into the cable systems that could be used to hinder or halt (when there is no option for rerouting) work in the EU and NATO bases either during the continued war in Europe or potential conflict in the Indo-Pacific. The kill switch-related risk is particularly high as the HMN controlling shareholder has cooperated with the PLA cyber intelligence affiliated institute on industrial control systems governing the work of modern infrastructure.

Neither would the French nor the Danish models mitigate any risks in the case of HMN. The cable system supplier, HMN, is an unreliable guarantor of its operational security due to factors mentioned earlier: the Chinese legal framework; parent company ties to the PLA; and participation in an MCF framework. Neither could cable system owners, telecom companies or individual Member States be made responsible for the security of HMN-provided systems as they are likely to lack the necessary skills and resources. For owners and telecom companies, it is mostly a case of commercial decisions with little or no emphasis on security. Such decisions could also potentially have a negative impact on the share market's operation, such as in 2021 when the EU imposed tariffs on a company from the same Hengtong Group as HMN over dumping[131].

Inside the EU there are no known cases of an undersea cable project being halted due to security concerns. FDI screening mechanisms would not prevent Chinese companies from building strategic infrastructure as the owner of the cable systems are in most cases local telecom companies. As explored earlier, the current NIS2 Directive adopted in January 2023 does not provide concrete measures for Member States regarding risk mitigation[132].

[126] Commission on the Defence Forces, Report of the Commission on the Defence Forces, February 2022, p. 35.
[127] C. Bueger, T. Liebetrau and J. Franken, 'Security threats to undersea communications cables and infrastructure – consequences for the EU', Policy Department for External Relations, PE 792.557, June 2022, pp. 37-38.
[128] French Ministry of Army, Seabed Warfare Strategy, Report by the Working Group, February 2022, p. 33.
[129] R. Kaljula, 'Hangxin's Acquisition – A Threat to EU Aviation Competitiveness', *Analysis*, 27 March 2023.
[130] R. Kaljula, 'Hangxin's Acquisition – A Threat to EU Aviation Competitiveness', *Analysis*, 27 March 2023, p. 39.
[131] R. Daws, 'EU to slap large tariffs on Chinese optical fibre cables', *Telecoms*, 19 November 2021.
[132] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), Official Journal of the European Union, L333/80, 27 December 2022.

5 Policy implications and recommendations

This In-depth analysis has used new research on China's access to EU critical infrastructure to identify risks that pose unique challenges to current regulatory instruments. While these risk categories are generally known within the regulatory framework, some of these risks' vectors appear to bypass its current and possibly future implementation.

5.1 Summary of risks and their mitigation under the current framework

Surveillance and espionage. Europe's critical infrastructure includes logistical nodes and telecommunications systems. Up-to-date information about their functionalities and vulnerabilities can provide 'adversaries' with critical advantages in both hybrid and overt confrontational scenarios. Within the Chinese political system, security agencies and the military can demand cooperation from state and privately-owned companies with intelligence collection efforts, a relationship made explicit in the 2017 Intelligence Law. The involvement of China investors and contractors in EU critical assets, such as ports and undersea cables, thus directly exposes Member States and their allies to the collection of intelligence by China. FDI-screening processes may exclude such actors from future sales or tenders only in a haphazard manner because the screening process is subject to individual Member States' own standards and voluntary adherence to EU-wide regulatory guidance. As a result, current vulnerabilities, such as China FDIs in European ports and Chinese contractors in undersea cable projects, cannot be mitigated without additional regulatory intervention.

Technology transfer to China's military. EU Member States possess unique abilities to develop and produce advanced technologies and strategic materials. Under the CCP's MCF strategy, Chinese civilian businesses and research institutions collaborate with the PLA, incentivising the sharing of research and development results between market-oriented and defence industries. The involvement of Chinese companies in EU strategic assets, especially companies that have direct or indirect links to China's defence system, entails a risk that technology and technological expertise will ultimately be transferred to China's military. The EU's current regulatory framework does not consider the unique characteristics of China's MCF, which offers incentives for technology transfer on a scale that may lack equivalents in other third countries. Only the exclusion of Chinese entities – most pressingly, those with documented links to China's defence systems – from any access to EU critical infrastructure may mitigate this risk. In the case of investors, such exclusion is possible under the current framework, yet subject to Member State implementation.

Strategic policy obstruction. As global powers, the EU and China see critical assets as tools serving competing strategies. Chinese companies' leverage on EU critical infrastructure, exerted through investment or other involvement, translates into leverage for the party-state. Owners or operators of EU strategic assets subject to China government leverage may be pressured to alter their business plans to conform to the needs of the Chinese government while abiding by the EU and Member State regulations as well as contracts with clients and suppliers. For example, the owners of strategic raw mineral mining licences or processing plants may prioritise procurement from, or sales to, China's market, or de-prioritise the production of materials needed by Europe's defence industry. In such situations, EU and Member State agencies have no mechanisms for significantly influencing owners' or operators' business decisions. This risk can be mitigated only by reducing China's leverage on entities involved in critical infrastructure. The current regulatory framework may effectively exclude certain Chinese investors from critical infrastructure projects. However, due to inconsistent implementation, they may not be able to address current and foreseeable future risks adequately.

Direct political influence. When entities controlled by the Chinese party-state gain prominent roles in EU critical infrastructure projects, the CCP becomes a stakeholder in European political processes, at EU, national and subnational levels. The CCP uses an array of dedicated agencies across its security, foreign

affairs, propaganda, 'united front' and economic bureaucracies, along with the party-controlled military and guided private sector, to co-opt and influence foreign elites, a setup that has no direct equivalent in non-Leninist political systems. Local authorities, down to city governments, that benefit from the presence of Chinese actors in critical infrastructure projects may be pressured into aligning themselves with China's policy goals, undermining the integrity of Europe's democratic systems. The risk of direct political influence can be mitigated by limiting significant ownership or other participation in European assets by China state entities. Their exclusion from future acquisition or tender processes may be enabled by the current regulatory framework. However, its implementation remains subject to Member-State decisions and may not be sufficient to counter leverage through mechanisms other than direct investment.

Indirect political influence. Political influence acts at a distance, using Chinese and non-Chinese private businesses as intermediaries on which the party-state exerts significant leverage. One case study demonstrated that a key node producing materials of strategic significance for Europe's defence industry is linked to a mining magnate who has vocally espoused China's propaganda narratives that contradict efforts by the EU and its allies to counter disinformation. The current regulatory framework makes it even harder to mitigate indirect than direct political influence risks, lacking an explicit concept of authoritarian leverage on private actors.

Cooperation with Russia. China is Russia's sole ally with global power-projection capabilities. The Russian invasion of Ukraine coincided with an unprecedented consolidation of the China-Russia alliance, which has clearly demonstrated Putin's authoritarian leadership adhering to the CCP's geopolitical initiative. NATO has repeatedly warned about the risks of China supporting Russia's war efforts in Ukraine, including the provision of weapons technology and intelligence cooperation. Against this backdrop, to the extent that access to EU critical infrastructure may aid China's intelligence and technology acquisition efforts, the risk must be considered that such information may be covertly shared with China's allies such as Russia, thus aiding them against Ukraine.

5.2 Policy recommendations: towards a unified critical infrastructure protection framework

The case studies demonstrate that threats to critical infrastructure are not limited to direct investment by China's state-owned companies. Even in such typical scenarios, the EU's investment-screening regulations, which were established recently and are still unevenly enforced, allow China to gain ownership stakes in critical assets. In other cases, where there are fewer direct links to the party-state, China may have even greater leverage on infrastructure projects due to insufficiently exhaustive screening procedures that fail to provide a proper assessment. Furthermore, in addition to investment, other forms of access through infrastructure, such as contractors, pose similar threats. This section suggests actions that can be taken by the EP and other stakeholders to address these threats.

Track and assess China's access to critical infrastructure in the EU. European Parliament Committees responsible for defence, security and political interference, such as the SEDE committee, should closely monitor China-linked entities' involvement in the EU's critical infrastructure. This can be achieved by conducting regular hearings and commissioning original research, with the knowledge and expert opinions on potential risks subsequently being made available to Member States' citizens. This will help to identify the risks that arise from critical assets being partially owned, operated, maintained, or accessed by entities over which the China party-state can exert significant leverage.

Strengthen FDI-screening procedures with due-diligence standards to identify China's leverage on investors in critical infrastructure. The EP should supplement existing investment regulations with explicit guidelines defining due-diligence standards to be applied when screening foreign investors. Since higher risk levels arise from investment in critical infrastructure, these standards should be more stringent in those cases. Such standards should not only assess whether China entities would ultimately own shares

in an EU asset, but also measure the extent of China party-state's leverage on prospective investors. This should consider channels such as market dependence and partnerships with Chinese entities. Standards should further define due diligence quality baselines; in particular, due diligence processes should incorporate Chinese-language research based on proven expertise on the China party-state and its links to private business, to avoid missing political connections through more superficial analytical methodologies.

Unify critical-infrastructure protection regulations by generalising investment and subsidy regulations, to include all forms of China's leverage on critical infrastructure, including contractors. The European Parliament should pass regulations expanding current instruments that address foreign direct investment and foreign subsidies to generalise screening procedures to all actors involved in EU critical infrastructure projects. Specifically, this should include contractors. These generalised regulations should be revised to establish explicit standards such as those described above.

Integrate EU regulations applicable to China entities, such as sanctions, into critical infrastructure protection regulations. The EU has imposed sanctions on Chinese entities linked to human rights abuses. Links to such entities should be considered when screening investors, contractors and other entities involved in critical infrastructure. The EP should consolidate sanctions regimes and related regulations into the critical-infrastructure protection framework.

Raise awareness of the risks to critical infrastructure among Member-State stakeholders. Through the public hearings of relevant EP committees, including the SEDE committee, and within Member States, MEPs should communicate their views on critical-infrastructure protection to Member-State stakeholders. A public consultation process initiated by the EP with relevant stakeholders from Member States' governments, industry, academia, EU institutions, business circles and the security community could not only increase awareness but also provide invaluable input for amendment of the FDI screening mechanism.

Coordinate critical-infrastructure protection at EU and national levels. Responsibility for protecting critical infrastructure ultimately lies with Member States, which should enact critical-infrastructure protection regulations consistent with those in force at EU level. In turn, relevant EP agencies and committees, including the SEDE committee, should track the development of Member-State critical infrastructure-protection frameworks, considering incorporating aspects of them as best practices into public communications and recommendations to update EU regulations.

References

Anderlini J. and Goujard C., 'Brussels moves to ban Eurocrats from using TikTok', *POLITICO*, 23 February 2023.

Asset Management Association of China, '私募基金管理人公示信息', Information announcement, 8 April 2023 [web archive]

Association of China Rare Earth Industry, '日立金属专利被判无效 稀土产业联盟告捷', 25 February 2016 [web archive].

Borrell, J. 'How to deal with China', The European External Action Service, 17 May 2023.

Bradsher K., 'Amid Tension, China Blocks Vital Exports to Japan', *New York Times*, 22 September 2010.

Brodsky, P. 'Content Providers Binge on Global Bandwidth ', *TeleGeography Blog*, 22 June 2022.

Brzozowski, A. 'EU expected to take a tougher stance on China', *Euractiv,* 17 October 2022.

Bueger C., Liebetrau T. and Franken J., 'Security threats to undersea communications cables and infrastructure – consequences for the EU', Policy Department of the European Parliament, PE 702.557, June 2022.

Caijing, '中国钕铁硼出口遭日本专利壁垒', 14 July 2014 [web archive].

Camesasca P., Henschen H., Kingsbury K. and Juhasz M., 'Foreign Direct Investment Regulation: EU M&A after one year of the FDI Regulation', *Covington,* 17 December 2021.

China Association or International Friendly Contact, 'Honorary Chairman Xu Kuangdi Meets with the Business Leaders from Australia', 29 July 2012.

China Association or International Friendly Contact, 'Vice-chairman Deng Rong Meets with Guests from Australia', 9 April 2013.

China Merchant Port, We connect the world, Interim report, 2020.

China Ministry of Industry and Information Technology, '稀土行业发展规划（2016-2020年）', 18 October 2016.

China Times, '中投：千亿资金转向能源资源领域', 7 December 2009 [web archive].

Chinese People's Political Consultative Conference, '中国人民政治协商会议第十三届全国委员会委员名单', 11 May 2020.

CK Hutchinson Holding, Solid • Resilient Resilient Ready for Tomorrow: 2021 Annual Report, 11 April 2022.

Commission on the Defence Forces, Report of the Commission on the Defence Forces, February 2022.

Council Decision (CFSP) 2021/481 of 22 March 2021 amending Decision (CFSP) 2020/1999 concerning restrictive measures against serious human rights violations and abuses, Official Journal of the European Union, LI 99/1, 22 March 2021.

Cristiani D., Ohlberg M., Parello-Plesner J. and Small A., 'The Security Implications of Chinese Infrastructure Investment in Europe', *The German Marshall Fund of the US*, Washington, DC, 28 September 2021.

Daws R., 'EU to slap large tariffs on Chinese optical fibre cables', *Telecoms*, 19 November 2021.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), Official Journal of the European Union, L333/80, 27 December 2022.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)', Official Journal of the European Union, L 333/164, 27 December 2022.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance), Official Journal of the European Union, L 333/164, 27 December 2022.

Doffman Z., 'Huawei Employees Linked To China's Military And Intelligence, Reports Claim', *Forbes*, 6 July 2019.

Duchâtel M. and Sheldon-Duplaix A., 'Blue China: Navigating the Maritime Silk Road to Europe', *European Council on Foreign Relations*, 23 April 2018.

Eesti Rahvusringhääling, 'Silmet owner to construct €100 million magnet factory in Narva', 9 November 2022.

Embassy of the People's Republic of China in Malaysia, '中共中央关于党的百年奋斗重大成就和历史经验的决议（全文）', 16 November 2021.

Emmott R., 'EU's statement on South China Sea reflects divisions', *Reuters*, 15 July 2016.

Erbel M. and Kinsey C., 'Think again – supplying war: Reappraising military logistics and its centrality to strategy and war', *Journal of Strategic Studies,* Vol 41, No 4, December 2015.

Estonian government, 'Valitsuse pressikonverents, 10. november 2022', Press release, 10 November 2022.

Euronews and *Associated Press*, 'Which countries have banned TikTok and why?', 4 April 2023.

European Commission, 'Speech by President von der Leyen on EU-China relations to the Mercator Institute for China Studies and the European Policy Centre', SPEECH/23/2063, 30 March 2023.

European Commission, 'Commission strengthens cybersecurity and suspends the use of TikTok on its corporate devices', Press Release, 23 February 2023.

European Commission, 'EU requests two WTO panels against China: trade restrictions on Lithuania and high-tech patents', IP/22/7528, 7 December 2022.

European Commission, 'Critical Infrastructure: Commission accelerates work to build up European resilience', Press Release, IP/22/6238, 18 October 2022.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2022) 548 final, 18 October 2022.

European Commission, 'International Ocean Governance: an agenda for the future of our oceans', 26 February 2021.

European Commission, Critical Raw Materials Resilience: Charting a Path towards greater Security and Sustainability, COM(2020) 474 final, European Commission, 3 September 2020.

European Parliament, List of screening mechanisms notified by Member States, last updated on 2 February 2023.

European Parliament, 'MEPs approve new rules to protect essential infrastructure', Press Release, 22 November 2022.

European Parliament, Report on foreign interference in all democratic processes in the European Union, including disinformation, Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, 2020/2268(INI), 8 February 2022.

Eurostat, 'Use of digital technologies among EU enterprises', 20 January 2022.

Federal Communications Commission, 'Submarine Cable Landing Licenses', n.d.

Fortescue, 'Fortescue Metals Group steps up as a strategic partner of the 2021 Boao Forum for Asia', News, 21 April 2021 [web archive].

Fortescue, 'Fortescue to be Diamond Partner of the 2020 Boao Forum for Asia', News, 16 January 2020 [web archive].

French Ministry of Army, Seabed Warfare Strategy, Report by the Working Group, February 2022.

Fritz A., 'The foundation for innovation under military-civil fusion: The role of universities', *Sinopsis*, 8 October 2021.

Gaens B., Jüris F. and Raik K. (eds.), *Nordic-Baltic Connectivity with Asia via the Arctic: Assessing Opportunities and Risks*, International Centre for Defence and Security, 2021.

Garnaut J., 'Australia's China reset', *The Monthly*, August 2018.

Garnaut, J. 'Chinese military woos big business', *Sydney Morning Herald*, 25 May 2013.

Groeneveld L. and Pankowska M., 'NATO in deep water because of chinese port investments', *Vsquare*, 18 October 2022.

Groeneveld L. and Pankowska M., 'NATO in deep water because of chinese port investments', *Vsquare*, 18 October 2022.

Hála, M and Lulu, J. 'Huawei's Christmas battle for Central Europe', *Sinopsis*, 28 December 2018.

Hála, M., 'United Front Work by Other Means: China's "Economic Diplomacy" in Central and Eastern Europe', *Jamestown Foundation*, China Brief, Vol 19, No 9, 9 May 2019.

Hallberg J., 'Foreign investment screening in Finland, Norway, Sweden and Denmark', in S. Hindelang and A. Moberg (eds), *Common European law on investment screening*, Springer, 2021, pp. 209–226.

Hamilton D. and Quinlan J., 'Chapter 5: The Digital Drivers of the Transatlantic Economy' in *The Transatlantic Economy 2023: Annual Survey of Jobs, Trade and Investment between the United States and Europe*, Washington, DC: Foreign Policy Institute, Johns Hopkins University.

Hanemann T. and Huotari M., 'Chinese FDI in Europe and Germany Preparing for a New Era of Chinese Capital', *Mercator Institute for China Studies and Rhodium Group*, June 2015.

Hellström J., Almén O., and Englund J., Chinese corporate acquisitions in Sweden: A survey, *Swedish Defence Research Agency*, February 2021.

Hengtong Group, '亨通成立未来工控系统信息安全国家级联合实验室', 7 May 2018.

Henley L. D., 'China Maritime Report No. 21: Civilian Shipping and Maritime Militia: The Logistics Backbone of a Taiwan Invasion', *China Maritime Studies Institute*, May 2022.

HMN Technologies, 'Huawei Marine Networks Rebrands as HMN Technologies', Press release, 3 November 2022 [web archive].

Jalinous F., Mildorf K. and Schomig K., '"Team Telecom" Formalized into New Committee; Increased Scrutiny of Chinese Involvement in US Telecommunications Services Continues', *White & Case,* 15 April 2020.

Jirouš F. and Lulu, J., 'Huawei in CEE: From "strategic partner" to potential threat', *Sinopsis*, 17 May 2019.

Joint Communication to the European Parliament, the European Council and the Council. EU-China – A strategic outlook, JOIN (2019) 5 Final, 12 March 2019.

Jüris, F., ' Sino-Russian Scientific Cooperation in the Arctic: From Deep Sea to Deep Space', in S. Kirchberger, S. Sinjen and N. Wörmer (eds), *Russia-China Relations: Emerging Alliance or Eternal Rivals?,* Springer, 2022, p. 185-202.

Jüris F., 'Estonia's Evolving Threat Perception of China', *The Prospect Foundation,* Prospects & Perspectives, No 25, 26 April 2022.

Jüris F., 'Handing over infrastructure for China's strategic objectives: 'Arctic Connect' and the Digital Silk Road in the Arctic', *Sinopsis*, 7 March 2020.

Jüris, F., 'The Talsinki Tunnel: Channelling Chinese Interests into the Baltic Sea', *International Centre for Defence and Security*, 2019.

Kaljula R., 'Europe's Port of Contention', commentary, *International Center for Defense and Security*, 26 October 2022.

Kaljula R., 'Hangxin's Acquisition – A Threat to EU Aviation Competitiveness', Analysis, 27 March 2023.

Kardon I. B. and Leutert W., Pier Competitor: China's Power Position in Global Ports, *International Security*, Vol 46, No 4, 2022.

Ker P. and Thompson B., 'Forrest pumps $150m into rare earths aspirant', *Australian Financial Review*, 26 August 2022.

Kono K. and De Tomas Colatin, S., 'National Approaches to the Supply Chain Cybersecurity: Taking a More Restrictive Stance Against High-Risk Vendors', *NATO Cooperative Cyber Defence Centre of Excellence*, 2023.

Kratz A., Zenglein M. J., Sebastian G. and Witzke M., 'Chinese FDI in Europe 2021 Update: Investments remain on downward trajectory-Focus on venture capital', *Mercator Institute for China Studies*, 27 April 2022.

Lee, R., Luttrell, P., Johnson, M. and Garnaut, J., 'TikTok, ByteDance, and their ties to the Chinese Communist Party', *Submission to the Australian Senate Select Committee on Foreign Interference through Social Media*, 14 March 2023.

Lee M., 'Top China college in focus with ties to army's cyber-spying unit', *Reuters,* 24 March 2013.

Liaowang Institute, '中国的稀土有多重要？', 21 May 2019 [web archive].

Lipman A. D., Pin U. R., and Weiss L., 'Protecting Submarine Cable Data Team Telecom Expanding its Toolkit to Include New Mitigation Measures', *Submarine Telecoms Forum Magazine*, 31 March 2022.

Macdonald A., Thompson S. and Sood K. 'Hastings Tech Metals readies $100m-odd raise after Wyloo investment', *The Australian Financial Review*, 5 September 2022.

Maiden S., 'Scott Morrison hits out at suggestion by Andrew 'Twiggy' Forrest COVID-19 could have originated in Australia', *News.com.au*, 1 May 2020.

Martin M., 'China in Greenland: Mines, Science, and Nods to Independence', *China Brief*, Vol 18, No 4, 12 March 2018.

Milbank, 'Milbank Represents Oaktree Capital Management in Successful Reorganization of Molycorp, Inc.', 1 April 2016 [web archive].

Mining Engineering, 'Molycorp completes work on its Phoenix Project, names new CEO', 9 October 2013 [web archive].

Mining Technology, 'Hastings acquires stake in Neo Performance Materials for $97m', 14 October 2022.

National People's Congress, '中华人民共和国国防交通法', 3 September 2016.

Neagu C., 'Industrial Control System (ICS): Definition, Types, Security', *Heimdal,* 8 February 2023.

Neo Performance Materials, 'Neo Performance Materials to Receive First-Ever Grant Under Europe's Just Transition Fund for Neo's Planned Sintered Rare Earth Magnet Manufacturing Plant in Estonia', 9 November 2022.

News.bjx.com.cn, '亨通海底观测网受中央军委、国防部等领导关注与好评', 25 September 2017.

Oaktree Capital Group, 'Oaktree and China Cinda Asset Management Announce Joint Venture', 25 November 2013 [web archive]; *Caixin*, '信达与橡树资本共同投资中国不良资产', 26 November 2013 [web archive].

Olsson J., 'China's Bid to Build the Largest Port in Scandinavia Raises Security Concerns', *Taiwan Sentinel*, 22 December 2017; C. B. Perlenberg, 'Låt inte Lysekil bli ett nordiskt', Troja, *Expressen*, 20 December 2017.

Open Source Center, Huawei Annual Report Details Directors, Supervisory Board for First Time, 5 October 2011.

People.com.cn, '胡锦涛在中国共产党第十八次全国代表大会上的报告', 人 民 网, 18 November 2012.

People's Daily, '习近平:深入实施军民融合发展战略 努力开创强军兴军新局面', 13 March 2015 [web archive].

Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, Official Journal of the European Union, LI 79/1, 21 March 2019.

Regulation (EU) 2022/2560 of the European Parliament and of the Council of 14 December 2022 on foreign subsidies distorting the internal market, Official Journal of the European Union, L 330/1, 23 December 2022.

Report from the Commission to the European Parliament and the Council Second Annual Report on the screening of foreign direct investments into the Union, COM(2022)433, Directorate-General for Trade, 1 September 2022.

Rinaldi G. and Wilke P., Germany rethinks China's Hamburg port deal as further doubts raised, *Politico*, 19 April 2023.

Robin M., 'Where did COVID-19 come from? Don't ask Twiggy Forrest', *Australian Financial Review*, 3 April 2020.

Roonemaa H., Eesmaa M., Liepina I., Bērzina S. and Navakas N., 'Hiina luure võtab Eesti üha jõulisemalt sihikule', *Postimees,* 5 September 2019.

Rühlig T., Jerdén B., Van der Putten F.P., Seaman J., Otero-Iglesias M. and Ekman A., Political values in Europe-China relations, report, *European Think-tank Network on China*, December 2018.

Seaman J., Huotari M., and Otero-Iglesias M., Chinese Investment in Europe: A Country-Level Approach, Report, *European Think-tank Network on China*, December 2017.

Shanghai Securities Journal via *Economic Daily*, '中投将向橡树资本投资10亿美元 双方都保持低调', 28 September 2009 [web archive].

Sims J., 'Letter: This mining facility is not as rare as we thought', *Financial Times*, 28 January 2021.

Sohu, ' 重磅 | 亨通成立未来工控系统信息安全国家级联合实验室 ', 6 July 2017 [web archive].

Starosielski, N., *The Undersea Network: against the flow*, Duke University Press, 2015

Stokes M. and Hsiao R., 'The People" s Liberation Army General Political Department: Political Warfare with Chinese Characteristics', Project 2049, 14 October 2013.

Stokes M. and Hsiao R., 'Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests', *Project 2049 Institute*, 29 October 2012.

Stoke, M. and Hsiao, R., 'The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics', *Project 2049 Institute*, 14 October 2013.

Stone A., and Wood P., *China's Military-Civil Fusion Strategy: A View from Chinese Strategists*, *China Aerospace Studies Institute*.

Submarine Telecoms Forum, 'Submarine Telecoms Industry Report 2022-2023', Vol 11, 2022.

Tabeta S., 'China weighs export ban for rare-earth magnet tech', *Nikkei*, 6 April 2023.

Tatlow D. K., 'China's Stake in World Ports Sharpens Attention on Political Influence', *Newsweek Magazine*, 10 September 2022.

The State Council Information Office, 'China's Military Strategy', *Ministry of National Defense of the People's Republic of China*, White Paper, May 2015.

Thorne D. and Spevack B., 'Harbored Ambitions: How China's Port Investments Are Strategically Reshaping the Indo-Pacific', C4ADS innovation for peace, 17 April 2018.

Tkacik J., 'Magnequench: CFIUS and China's Thirst for U.S. Defense Technology', *Heritage Foundation*, 2 May 2008; *South China Morning Post,* 'Onfem in US magnetic', 7 January 1997 [web archive].

Topf A., 'Mountain Pass sells for $20.5 million', *Mining.com*, 16 June 2017.

UK government, 'National Security and Investment Act 2021', *UK Public General Acts*, 2021.

US Code, '47 USC 34: Licenses for landing or operating cables connecting United States with foreign country; necessity for', Title 47-Telecommunicationschapter 2-Submarine Cables, Office of the Law Revision Counsel, laws in effect on 26 April 2023.

US Department of Defense, Military and Security Developments Involving the People's Republic of China 2022, report to Congress, 29 November 2022.

US Department of Justice, 'The Committee For The Assessment Of Foreign Participation In The United States Telecommunications Services Sector', n.d.

Wade G, 'Spying beyond the façade', *Australian Strategic Policy Institute*, 13 November 2013.

Wall C. and Morcos P., 'Invisible and Vital: Undersea Cables and Transatlantic Security', *Center for Strategic and International Studies,* 11 June 2021.

Weihua Z., '习近平时代的中国周边外交：新理念，新概念，新举措"研讨会综述', Seminar Summary of the 'China Periphery Diplomacy of the Xi Jinping Era: New Ideas, New Concepts, New Measures', *China International Studies*, Vol 1, 2015.

Wu T. and Hung C-L, 'Chapter 8 Cyber Warfare Capabilities of the PLA Strategic Support Force (SSF)', *Institute for National Defense and Security Research*, 2022.

Wyloo Metals, 'Wyloo Metals Invests $150 Million In Rare Earth Materials', 26 August 2022 [web archive].

PE 702.592
EP/EXPO/SEDE/FWC/2019-01/LOT4/3/C/15

Print ISBN 978-92-848-0859-5 | doi: 10.2861/987912 | QA-07-23-238-EN-C
PDF ISBN 978-92-848-0860-1 | doi: 10.2861/787684 | QA-07-23-238-EN-N