EU Strategic Autonomy and the Perceived Challenge of China: Can Critical Hubs Be De-weaponized?*

Tero POUTALA**, Elina SINKKONEN*** & Mikael MATTLIN****

Geoeconomic competition, supply security vulnerabilities and complex technological dependencies challenge the European Union's 'strategic autonomy'. Evolving from more traditional security/defence notions, a broader definition of strategic autonomy encompasses also economic dimensions. Economic resilience underpins security and defence arrangements. The EU has lacked instruments for protection against 'predatory' strategic investments by external actors, and technological dependence on potential strategic rivals. This article analyses two critical hubs, or potential 'chokepoints', in the EU's attempts to achieve strategic autonomy – critical maritime transport infrastructure and 5G – as well as countermeasures developed by the EU. Chinese enterprises have made strategic investments in key EU infrastructure and high-tech industries over the past decade. In response, the EU has established an investment screening framework to screen (authorize, issue condition, prohibit or unwind) inward foreign direct investment (FDI) on security or public order grounds, and activated a mechanism for the enhancement of coordination and cooperation between the Commission and Member States. The EU has also sought to reduce reliance on Chinese suppliers by introducing the '5G toolbox'. We argue that the EU aims to 'de-weaponize' these two potential chokepoints. However, our article concludes that the political goal of strategic autonomy vis-à-vis external actors is hampered by the competence limitations of the Union to act in critical areas. Ultimately, much of the heavy lifting on implementing EU policy goals still falls upon Members States with varied economic and security interests.

Keywords: chokepoint effects, critical hubs, strategic autonomy, interdependence, investment screening, 5G toolbox

1 STRIVING FOR STRATEGIC AUTONOMY IN AN AGE OF WEAPONIZED INTERDEPENDENCE

The European Union (EU) has in recent years strived for a measure of 'strategic autonomy', an aim first enshrined in the 2016 EU Global Strategy (EUGS).[1]

* The authors acknowledge financial support from the Academy of Finland (grant 338145).
** Doctoral Candidate at the University of Turku. Email: tero.p.poutala@utu.fi.
*** Senior Research Fellow at the Finnish Institute of International Affairs. Email: Elina.Sinkkonen@fiia.fi.
**** Professor of Political Science (act.) at the University of Turku. Email: mikael.mattlin@utu.fi.
1 European External Action Service, *Shared Vision, Common Action: A Stronger Union. A Global Strategy for the European Union's Foreign and Security Policy* (Publications Office of the European Union 2016).

Poutala, Tero; Sinkkonen, Elina & Mattlin, Mikael. 'EU Strategic Autonomy and the Perceived Challenge of China: Can Critical Hubs Be De-weaponized?'. *European Foreign Affairs Review* 27, Special Issue (2022): 79–98.

Strategic autonomy refers to efforts the EU makes to manage interdependencies with third parties encompassing all the EU's economic and political engagements.[2] The concept's connotations have gradually expanded from a rather narrow understanding pertaining mainly to the military sphere, to encompass broader remits. Yet, there are multiple competence issues between the EU and its Member States hindering the Union from reaching strategic autonomy.

One key area of strategic autonomy concerns technological dependencies. China's technological innovation and emergence as a leader in fields such as artificial intelligence and fifth generation mobile technologies (5G) pose challenges for the EU's efforts to maintain technological sovereignty and retain global regulatory power.[3] In the 2021 State of the Union Address, European Commission President Ursula von der Leyen stressed the need to invest in European technological sovereignty 'to shape our digital transformation according to our own rules and values'. The same speech announced a new initiative, the European Chips Act, which aims to decrease European dependence on semiconductors.[4] Early 2022, the Commission called for digital sovereignty over semiconductors, and communicated related regulation proposals and the semiconductor toolbox.[5]

The discussion on strategic autonomy inevitably touches on perceived risks associated with excessive reliance on large external state actors. Usually this signifies authoritarian states such as Russia and China. However, the EU also has security dependencies on the United States that de facto reduce its strategic autonomy, even though these dependencies are not generally perceived as threatening as, e.g., high reliance on Russian gas that can be exploited for geostrategic aims,[6] or Chinese investments in critical infrastructure.[7]

That interdependencies can also be a vulnerability, in addition to having benign effects, is not a novel idea. Hirschman first suggested that states may use asymmetric trade relations as a source of power.[8] Later Keohane and Nye, who are widely credited for bringing the interdependence discussion to international relations theory

---

2 N. Helwig, *EU Strategic Autonomy: A Reality Check for Europe's Global Agenda*, 119 FIIA Working Paper (2020).

3 T. Gehrke, *EU Open Strategic Autonomy and the Trappings of Geoeconomics*, 27 Eur. For Affairs Rev. Special Issue (2022); Q. Levin, *A Review of the Brussels Effect*, 22(2) Geo. J. Intl. Affairs 307–310 (2021).

4 European Commission, *2021 State of the Union Address by President von der Leyen*, SPEECH/21/4701, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701 (accessed 29 Nov. 2021).

5 European Commission, *Digital Sovereignty: Commission Proposes Chips Act to Confront Semiconductor Shortages and Strengthen Europe's Technological Leadership*, IP/22/729, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_729 (accessed 10 Feb. 2022).

6 For example M. Wigell & M. & A. Vihma, *Geopolitics Versus Geo-Economics: The Case of Russia's Geostrategy and Its Effects on the EU*, 92(3) Intl. Affairs 605–627 (2016).

7 For example, J. Seaman, *Towards a more China-centred Global Economy? Implications for Chinese Power in the Age of Hybrid Threats*, Hybrid CoE Paper, no. 9, European Centre of Excellence for Countering Hybrid Threats (Nov. 2021).

8 A. Hirschman, *National Power and the Structure of Foreign Trade* (University of California Press 1945).

in the 1970s, discussed asymmetrical interdependence, dependencies, and vulnerabilities.[9] Gilpin noted that dissemination of technology under a liberal hegemon eventually leads to challenges to the hegemon that, in turn, spur mercantilist responses.[10] Later, Luttwak discussed how the 'logic of conflict' was embedded in the 'grammar of commerce',[11] while Crawford talked of the 'economic security dilemma' inherent in globalized production and exchange networks in the context of states that continue to strive for security through military means.[12]

This paper takes its cue from the seminal article[13] by Farrell and Newman on 'weaponized interdependence'. They argue that complex systems tend to form asymmetric network structures that give disproportionate power to actors in control of critical network hubs, making it possible to weaponize interdependence on a systemic level without feeling the consequences. As Farrell and Newman argue, interdependence can be weaponized in two different ways through the *panopticon* effect or the *chokepoint* effect. The former refers to 'advantaged states using their network position to extract informational advantages vis-à-vis adversaries, whereas in the latter, they can cut adversaries off from the network'. As a historical precedent for a chokepoint, Farrell and Newman gave the example of the United Kingdom, which before World War I had a near monopoly on international communications and had developed extensive plans for disrupting the economies of its enemies through these networks. More recently, the United States has similarly dominated information networks, although it has been less eager to use them as chokepoints, because of the commercial benefits accruing to it from open networks.[14]

In this article, we focus our attention on the potential chokepoint effects of Chinese investments in EU critical port infrastructure and 5G networks. While China is not one of the largest investors in the EU, its authoritarian political system and the perceived close connections between the Chinese state and Chinese economic actors make it qualitatively different as an investor. Chinese infrastructure investments in the EU are typically done by the just under 100 large business groups that are called 'central enterprises' (中央企业)—state-owned enterprises (SOE) administered by the State-Owned Assets Supervision and Administration

---

9 R. O. Keohane & J. S. Nye Jr., *Power and Interdependence Revisited*, 41(4) Intl. Org. 725–753 (1987).

10 R. Gilpin, *Economic Interdependence and National Security in Historical Perspective*, in *Economic Issues and National Security* (K. Knorr & F. N. Trager eds, Regents Press of Kansas 1978); Gehrke, *supra* n. 3.

11 E. N. Luttwak, *From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce*, 7(5) Intl. Economy 18–67 (1990).

12 B. Crawford, *The New Security Dilemma Under International Economic Interdependence*, 23(1) Millennium J. Intl. Stud. 25–55 (1994).

13 H. Farrell & A. L. Newman, *Weaponized Interdependence. How Global Economic Networks Shape State Coercion*, 44(1) Intl. Sec. 42–79 (2019).

14 *Ibid*.; N. A. Lambert, *Planning Armageddon: British Economic Warfare and the First World War* (Harvard University Press 2012).

Commission (SASAC) under the Chinese State Council.[15] Given this special status, it is reasonable to assume that they are at least sensitive to political guidance.

However, even nominally non-SOE Chinese companies have raised suspicions in the West due to their often-opaque corporate governance structures. Exacerbating the concern are the increasingly deep interlinkages between the economy and national security in China over the past decade. China, e.g., actively pursues civil-military integration and its' recent economic policies have been strongly security-oriented. Furthermore, the 2017 National Intelligence Law compels all Chinese organizations and citizens to comply with Chinese intelligence efforts. Increasing great power competition makes the EU's position even more difficult, as technological decoupling between the United States (US) and China can pressure Europe to choose sides. The US restricts Chinese investments in security-relevant fields inter alia through the Committee on Foreign Investment of the United States (CFIUS).

Empirically, our article delves into how Chinese investments in critical port infrastructure and technological dependence on Chinese 5G suppliers have prompted concern and countermeasures in the EU. These sectors cover thematically both the EU's physical and technological autonomy. The sectors were chosen because they have figured prominently in the security debate. Port infrastructures are the physical enablers of international transport of goods and passengers by sea, while information technologies facilitate everyday work, communication, and governance of physical activities. 5G is the newest information technology standard. Not only do port infrastructure and 5G form critical infrastructure separately, but port infrastructures rely increasingly on data transfers through 5G networks. The main rationale for choosing 5G as a case study is that many critical services depend on it and will do so even more in the future. 5G connects physical and virtual reality. Without control over its telecommunication networks supporting everyday life and business, the EU would not be able to achieve its goal of strategic autonomy. 5G has been identified as a key asset for Europe.[16] Corporate takeovers and a strong market presence in these two sectors by third countries, such as China, therefore, pose a potential challenge. Both cases also showcase variance within the Union, as some countries welcome Chinese investments, whereas others are very sceptical towards them. Analysing these two key sectors highlights advancements and limitations in the EU's reaching strategic autonomy.

---

[15] *See* M. Mattlin, *Chinese Strategic State-Owned Enterprises and Ownership Control*, 4(6) BICCS Asia Papers, Brussels Institute of Contemporary China Studies, 1–28 (2009), for an account of how the SASAC administers central enterprises.

[16] European Commission, *Secure 5G Networks: Commission Endorses EU Toolbox and Sets Out Next Steps*, Press release, IP/20/123 (Brussels, 29 Jan. 2020).

The next section provides a brief overview of EU-China interdependencies. The third and fourth sections probe into the two case studies, while the fifth section examines the EU's arsenal of countermeasures in managing its interdependence. The final section summarizes the main findings of the study.

2 MANAGING INTERDEPENDENCIES IN EU-CHINA RELATIONS

The EU's relationship with China is complicated. The Union tries to balance its policies towards a China that is regarded simultaneously as a 'partner', 'competitor' and 'rival'. China is a growing market for the EU and a source of economic innovations, the importance of which are likely to increase in the future following China's large investments in future technologies.[17] Since 2020, the EU and China are each other's largest trading partners.[18] The EU also recognizes the need to cooperate with China on global issues such as climate change. Still, China's recent turn towards an increasingly state-driven 'dual circulation' economic model, has ushered in a sense of urgency in Europe and the US.[19] The EU characterization of China as also a 'systemic rival' emerged for the first time in March 2019.[20]

Over the past decade, Europe has seen a surge of Chinese FDI in various critical sectors, including energy and transport, with a cumulative value of tens of billions euros.[21] However, to put this in perspective, it still represents only a fraction of the EU's over EUR 10 trillion inward FDI stock, and only a small part of the EU's annual inward FDI flows that are typically several hundred billion. Even mid-sized European economies like Switzerland and Norway are bigger investors in the EU than China.[22]

---

17 It has been announced that China is bidding for global leadership in key technologies with more than a trillion euros in investment, from wireless networks to artificial intelligence. Bloomberg, *China Has a New $1.4 Trillion Plan to Overtake US in Tech* (20 May 2020), https://www.bloomberg.com/news/articles/2020-05-20/china-has-a-new-1-4-trillion-plan-to-overtake-the-u-s-in-tech (accessed 29 Nov. 2021).

18 European Commission, *Countries and Regions: China*, https://ec.europa.eu/trade/policy/countries-and-regions/countries/china/ (accessed 29 Nov. 2021); Politico, *China Topples US as EU's Top Trade Partner Over 2020* (15 Feb. 2021), https://www.politico.eu/article/china-topples-us-as-eus-top-trade-partner-over-2020/ (accessed 29 Nov. 2021).

19 *Business Europe, The EU and China: Addressing the Systemic Challenge: A Comprehensive EU Strategy to Rebalance the Relationship with China* (Jan. 2020).

20 European Commission, *Commission Reviews Relations with China, Proposes 10 Actions*, Press release, 12 (Mar. 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1605 (accessed 29 Nov. 2021).

21 For example, P. Pareja-Alcaraz, *Chinese Investments in Southern Europe's Energy Sectors: Similarities and Divergences in China's Strategies in Greece, Italy, Portugal and Spain*, 101 Energy Pol'y 700–710 (2017); Merics, *Chinese FDI in Europe 2020 Update: Investment Falls to 10-Year Low in an Economically and Politically Challenging Year*, Merics report (June 2021).

22 *See* e.g., about recent developments: European Commission, *Report from the Commission to the European Parliament and the Council: First Annual Report on the Screening of Foreign Direct Investments Into the Union*, COM(2021) 714 final, SWD(2021) 334 final, 3–4 (Brussels, 23 Nov. 2021).

Simultaneously with the strive for technological sovereignty, Chinese leader Xi Jinping's signature foreign economic policy, the Belt and Road Initiative (BRI), has raised concern about China's infrastructure financing and its underlying motivations. China's infrastructure investments in the EU have been particularly notable in ownership stakes in key European ports.[23] China has presented the BRI as an expression of its willingness to provide international public goods and to share international responsibilities.[24] Interconnectivity has by some observers been regarded as the primary purpose behind the BRI.[25] 18 EU Member States, including Italy and Portugal, have signed BRI agreements with China.[26]

Concerns related to Chinese infrastructure investment grew around the EU following a large jump in Chinese investment in 2015–16 and China's active promotion of its BRI projects, especially in Eastern Europe. Lack of 'reciprocity' on investments drew concern. The EU market was relatively open to foreign investors and lacking in government oversight, whereas it was much harder for European companies to complete similar investments in China.[27] This prompted calls from France, Germany, and Italy to introduce EU-wide investment screening.[28] In June 2017, the European Council urged the Commission to 'analyse investments from third countries in strategic sectors, while fully respecting Members States' competences'.[29]

3 CASE STUDY: INVESTMENTS IN CRITICAL PORT INFRASTRUCTURE

Ports typically consist of port facilities, infrastructure, operations, and transport connections. Many seaports can be classified as hubs, being 'crucial intermediaries

---

23 Merics, *COSCO Takes Stake in Hamburg Port Terminal* (30 Sept. 2021), https://merics.org/en/tracker/cosco-takes-stake-hamburg-port-terminal (accessed 29 Nov. 2021) .

24 Belt and Road Forum, *Building the Belt and Road for Win-Win Development,* http://www.beltandroadforum.org/english/n100/2017/0417/c25-195.html (accessed 29 Nov. 2021).

25 Z. H. Hu, C. J. Liu & P. T. W. Lee, *China's Global Investment and Maritime Flows in the Context of the Belt and Road Initiative*, 30(129) J. Contemp. China 465–480, 467 (2021).

26 Silk Road Briefing, *European Union Member States Who Joined China's Belt And Road Initiative Are Seeing Their Exports Rise Faster By Nearly 5% More Than Those Who Have Not*, https://www.silkroadbriefing.com/news/2020/11/20/european-union-Member-States-who-joined-chinas-belt-and-road-initiative-are-seeing-their-exports-rise-faster-by-nearly-5-more-than-those-who-have-not/ (accessed 29 Nov. 2021).

27 T. Hanemann & M. Huotari, *EU-China FDI: Working Towards Reciprocity in Investment Relations*, MERICS Papers on China, No. 3. Rhodium Group & MERICS (Berlin, 17 Apr. 2018), www.merics.org/sites/default/files/2018-08/180723_MERICS-COFDI-Update_final_0.pdf (accessed 20 Nov. 2021).

28 Reuters, *France, Germany, Italy Urge Rethink of FOREIGN INVESTMENT in EU* (14 Feb. 2017), https://www.reuters.com/article/uk-eu-trade-france-idUKKBN15T1ND (accessed 29 Nov. 2021).

29 European Council, *European Council Conclusions*, EUCO 8/17, 8 (Brussels, 23 June 2017), https://www.consilium.europa.eu/media/23985/22-23-euco-final-conclusions.pdf (accessed 29 Nov. 2021).

in decentralized communication structures'.[30] They form an integral part of global supply chains, the importance of which has been amply demonstrated by the post-Covid-19 supply problems that often culminate in clogged seaports. Since the EU is profoundly dependent on maritime transport for foreign trade, energy and its territorial continuity,[31] maritime transport infrastructures have monumental strategic importance.[32] The Commission has included transportation and mobility as 'sensitive ecosystems' of possible strategic dependency, i.e., having critical importance to the EU and its Member States' strategic interests.[33]

Firstly, ports require fairways to enable the safe movement of vessels with certain draught. Secondly, although there is a limited substitutability between ports nearby, typically fairways and other physical properties of ports do not make it easy or economical to change port operations to another place. Thirdly, many ports and fairways serve also military shipping purposes. Every port is somehow connected to the transport infrastructure of the mainland, ports being the nexus between those. More than 80% of world trade by volume is carried by sea.[34] In some countries, this ratio is even higher, e.g., around 90% of Finland's external trade is seaborne, i.e., passes through a port.[35]

The BRI has ushered in an expansion of Chinese ownership in European ports, mainly by China Communications Construction Company (CCCC), China Merchants Group (CMG) and China Ocean Shipping (COSCO)—all of which are party-state controlled central enterprises.[36] This includes significant stakes in more than a dozen ports, and around 10% of the European container port capacity. Around 65% of Chinese port investments are within the BRI framework.[37] There

---

30 Farrell & Newman, *supra* n. 13, at 55.

31 European Commission, *Ports 2030—Gateways for the Trans European Transport Network* (2013), https://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/site/brochures_images/ports2013_brochure_lowres.pdf (accessed 29 Nov. 2021).

32 *See* e.g., Council of the European Union, *European Union Maritime Security Strategy*, 11205/14, 2 (Brussels, 24 June 2014); *Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 Dec. 2013 on Union guidelines for the Development of the Trans-European Transport Network and Repealing Decision No 661/2010/EU*, Preamble 40, Arts 20 and 38(1).

33 European Commission, *Commission Staff Working Document - Strategic Dependencies and Capacities. Accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Updating the 2020 New Industrial Strategy: Building a Stronger Single Market for Europe's Recovery*, SWD(2021) 352 final, Graph 1 (Brussels, 5 May 2021).

34 United Nations Conference on Trade and Development, *Review of Maritime Transport*, 20 (United Nations Publications, UNCTAD/RMT/2020).

35 Finnish Shipowners' Association, *Key Figures of Maritime Transport in Finland*, https://shipowners.fi/en/competitiveness/key-figures-of-maritime-in-finland/ (accessed 29 Nov. 2021).

36 The Economist, *China Is Making Substantial Investment in Ports and Pipelines Worldwide*, Special report (6.Feb. 2020), https://www.economist.com/special-report/2020/02/06/china-is-making-substantial-investment-in-ports-and-pipelines-worldwide (accessed 29 Nov. 2021).

37 J. Chen, Y. Fei, P. T. W. Lee & X. Tao, *Overseas Port Investment Policy for China's Central and Local Governments in the Belt and Road Initiative*, 28(116) J. Contemp. China, 196–215, 202 (2019).

have been acquisitions, joint ventures, building, and expansion of European ports and terminals. Acquisitions, as an equity stake of company ownership, is the most-used action in Chinese foreign investments to obtain control.[38]

Most academic publications on Chinese investments relate to the economic rationale behind Chinese investments,[39] and investment screening mechanisms,[40] Less attention has been directed to the intersection between economic and security studies, and strategic autonomy. Security concerns include a lease agreement by China Logistics for 99 years of Jade-Weser-Port in Wilhelmshaven, Germany due to its proximity to the only German naval-based command in the North Sea.[41] COSCO has stakes in the ports of Piraeus and Rotterdam[42] and a terminal operator monopoly in Zeebrugge.[43] Since 2013, COSCO has had a special position among state-owned enterprises. Its' activities have spilled over to the security sphere and having its own militia has enabled COSCO to assist the People's Liberation Army Navy (PLAN) in the Gulf of Aden.[44]

---

38 W. Huo et al., *International Port Investment Of Chinese Port-Related Companies*, 11(5) Intl. J. Shipp Transp. Logist. 446 (2019).

39 *See* e.g., P. T. W. Lee, Z. H. Hu, S. J. Lee, K. S. Choi & S. H. Shin, *Research Trends and Agenda on the Belt and Road (B&R) Initiative with a Focus on Maritime Transport,* 45(3) Marit Policy Manag 282–300 (2018); Chen et al., *supra* n. 37; Z. Liu, S. Schindler & W. Liu, *Demystifying Chinese Overseas Investment in Infrastructure: Port Development, the Belt and Road Initiative and Regional Development*, 87 J. Transp. Geogr. (2020); Z. H. Hu, C. J. Liu, & P. T. W. Lee, *China's Global Investment and Maritime Flows in the Context of the Belt and Road Initiative*, 30(129) J. Contemp. China 465–480 (2021); W. Yin, *A Comparison of the US and EU Regulatory Responses to China's State Capitalism: Implication, Issue and Direction*, 19(1) Asia Eur. J. 1–25 (2021).

40 For example, B. Canes-Wrone, L. Mattioli & S. Meunier, *Foreign Direct Investment Screening and Congressional Backlash Politics in the United States*, 22(4) Br. J. Politics Intl. Rel. 666–678 (2020); S. Riela & P. Zamborsky, *Screening of Foreign Acquisitions and Trade in Critical Goods*, 18(3) Asia-Pacific J. EU Stud. 55–83 (2020); A. Ufimtseva, *The Rise of Foreign Direct Investment Regulation in Investment-Recipient Countries*, 11(2) Glob. Pol'y 222–232 (2020); S. F. Wernicke, *Investment Screening: The Return of Protectionism? A Business Perspective*, in YSEC Yearbook of Socio-Economic Constitutions, 29–41 (Springer, Cham. 2020); Z. T. Chan S. & Meunier, *Behind the Screen: Understanding National Support for a Foreign Investment Screening Mechanism in the European Union*, Rev. Intl. Org. (2021); G. Gertz, *Investment Screening Before, During, and After COVID-19*, 2(1) Glob. Perspect. (2021); S. Bauerle Danzman & S. Meunier, *The Big Screen: Mapping the Diffusion of Foreign Investment Screening Mechanisms* (28 Aug. 2021); E.g., G. Grieger, *Foreign Direct Investment Screening: A Debate in Light of China-EU FDI Flows*, EPRS, European Parliamentary Research Service, Members' Research Service (2017); P. Le Corre, *European and American Approaches Towards Chinese Foreign Direct Investment in Post-COVID Times: Opportunities, Challenges and Policy Responses*, in *Europe in an Era of Growing Sino-American Competition*, 138–154 (S. Biba & R. Wolf, Routledge 2021).

41 M. Ohlberg, *Germany and Its Neighbors*, in *The Security Implications of Chinese Infrastructure Investment in Europe* The German Marshall Fund of the United States, Report, 12 (D. Cristiani, M. Ohlberg, J. Parello-Plesner & A. Small eds, Sept. 2021).

42 On Oct. 2021, it was announced COSCO to divest its stake in Euromax Terminal (Rotterdam) to Navigator Investco, an Investment Platform for the Company and Silk Road Fund. *See* Seatrade Maritime News, *Cosco Sells Stake in Euromax Terminal to Investment Arm* (22 Oct. 2021), https://www.seatrade-maritime.com/ports-logistics/cosco-sells-stake-euromax-terminal-investment-arm (accessed 29 Nov. 2021).

43 Ohlberg, *supra* n. 41, at 12.

44 *Ibid*.

Some commentators have argued that Chinese influence in port infrastructure can lead to the compromising of national-level strategic autonomy by transforming economic dependence to political leverage.[45] Chinese port investments *per se* might not lead to economic dependence and Chinese political influence. However, taken in conjunction with Chinese dominance in container shipping, concentrated port investments can lead to such outcomes.[46] Huo et al. identified four characteristics regarding port investments by COSCO Shipping Ports: 1) ports are located on the main global trade routes; 2) the investments focus on existing ports; 3) a few of the investments have extended from earlier investments; and 4) most port investments have taken place since 2013, i.e., after the BRI was initiated.[47]

Although governing port infrastructure does not automatically indicate control over maritime routes, seen in this larger context, that may well be the end-result in specific situations, leading also to potential chokepoint effects. Each port has its own characteristics and physical connections. There is no economic rationale in shifting the physical location of a particular port.

Since ports are typically also hubs of international voyages, states have a physical presence there, e.g., being occupied by personnel and surveillance of border guards and customs. Various national expropriation mechanisms are often in place as a last resort measure to retain control over *tangible* port infrastructure if national security so requires. However, less attention has been given to the EU's strategic autonomy and competence in this context.

At present, the EU has not been conferred competencies, viz. capabilities to act and govern interdependencies, in the security and real estate domains to screen port investments. At the same time as the strategic importance of the seaports is evident, the varying economic interests of Member States can lead into a complex and asymmetric grid of investments and maritime-related dependencies. The fact that the EU does not have the capability to execute control over the ownership of seaports within the Member States raises the question of the possible level of strategic autonomy. It is questionable whether the EU has possibility to reach autonomy over the seaports and related infrastructure under the current umbrella of competencies, since ultimately the Union's autonomy is subject to cooperation between the Member States.

---

45 *See* e.g., F.-P. Van der Putten, *Chinese Investment in the Port of Piraeus, Greece: The Relevance for the EU and the Netherlands*, Clingendael Report (2014), https://www.clingendael.org/sites/default/files/pdfs/2014%20-%20Chinese%20investment%20in%20Piraeus%20-%20Clingendael%20Report.pdf; F.-P. Van der Putten, *European Seaports and Chinese Strategic Influence: The Relevance of the Maritime Silk Road for the Netherlands*, Clingendael Report (2019), https://www.clingendael.org/sites/default/files/2019-12/Report_European_ports_and_Chinese_influence_December_2019.pdf.

46 Van der Putten (2019), *supra* n. 45, at 15-17.

47 Huo et al., *supra* n. 38, at 436, 439.

4 CASE STUDY: 5G SUPPLIERS AND MARKET ACCESS

5G is a novel wireless mobile technology with utmost global importance, since it is estimated to connect at least 7 trillion wireless devices.[48] 5G mobile wireless technology provides high speeds/bandwidths and low latencies, which enable them to meet huge demand. The idea behind 5G is to connect physical infrastructure and devices together holistically via 5G hubs.

There is a fundamental difference between traditional port infrastructure and 5G. While port infrastructure can be categorized mainly as tangible infrastructure, 5G operates under both domains as a hybrid, i.e., as both tangible (e.g., devices) and intangible (e.g., software). However, one should not underestimate the importance of 5G networks and other technology aspects in relation to traditional maritime infrastructure. Port operations are increasingly being automated, as communication networks are a critical enabler in the ongoing technological transformation. Thus, we have seen increasing embedding of 5G into port infrastructure to enable their transformation into '5G smart ports'. For instance, Huawei has launched the Smart Port Solution to help build world-class ports.[49] The functions of these smart ports include increased situational awareness and overall connectivity between different port operators[50] and remote operations,[51] creating a chokepoint that, in theory, could be utilized by a Chinese state-actor for malignant purposes.[52]

5G concerns have similarly been closely related to China, as one of the main suppliers (Huawei) allegedly maintains close and opaque links to the Chinese state, including its military.[53] As the world's largest provider of communications technology, China occupies a central place in the 'network wars'.[54] By some accounts, China already leads the way to global standards for 5G and beyond.[55] Compared to its competitors, Huawei's strong point is its ability to produce all components in a

---

48 I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila & A. Gurtov, *Overview of 5G Security Challenges and Solutions*, 2(1) IEEE Communications Standards Magazine 36–43 (2018).

49 *See* Huawei, *Huawei Launches the Smart Port Solution to Help Build World-Class Ports*, 23 Sept. 2021, https://e.huawei.com/en/news/ebg/2021/smart-port-solution-help-build-world-class (accessed 29 Nov. 2021).

50 *See* e.g., S. Harris, *Private 5G: Enabling Ports of the Future*, Orange Business Services, https://www.orange-business.com/en/blogs/private-5g-enabling-ports-future (accessed 29 Nov. 2021).

51 Ericsson, *Smart Ports: At the Gateway to a New Shipping Age*, https://www.ericsson.com/en/industries/ports (accessed 29 Nov. 2021).

52 Seaman, *supra* n. 7.

53 B. Mascitelli & M. Chung, *Hue and Cry Over Huawei: Cold War Tensions, Security Threats or Anti-competitive Behaviour?*, 1Research in Globalization 1–6 (2019).

54 E. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (Haroper Business, 2021).

55 Financial Times, *China Leads the Way on Global Standards for 5G and Beyond*, 5 Aug. 2020, https://www.ft.com/content/858d81bd-c42c-404d-b30d-0be32a097f1c (accessed 29 Nov. 2021).

5G network supply chain in large quantities.[56] Preparations for 6G are also under way, with similar concerns to those of 5G.[57]

Provision of critical 5G infrastructure components makes it possible – at least in theory – to exploit the 5G hubs. 5G security risks can be outlined as unauthorized access or usage of assets.[58] Higher speeds enable exploitation of larger amounts of data and automated processes and operations can be vulnerable. Simultaneously, the increased number of interconnected devices and machines enables exploitation. Furthermore, the new Chinese legislation requiring Chinese citizens and companies to comply with the demands of the Chinese state for cooperation, has often been noted as a red flag.[59] Awareness and concern of China-related 5G-risks have been forcefully pushed by the US government, which has lobbied EU governments to take measures to exclude Chinese suppliers from European 5G networks and shun Chinese components in domains critical for national security.

In addition to surveillance concerns, technological competition also motivates the US, which regards Chinese efforts to create and promote their own technological ecosystems threatening, as they would undermine US ecosystems.[60] Consequently, the US goal has been to diminish its dependence on Chinese technology, with some success. The Trump administration's Clean Network Initiative was signed by nine EU Member States, mainly in Eastern Europe.[61] The Biden administration has given an executive order to strengthen domestic 'supply chains for critical sectors and subsectors of the information and communications technology (ICT) industrial base, including the industrial base for the development of ICT software, data, and associated services'.[62] In 2019, there was

---

56 T. Rühlig & M. Björk, *What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe*, UI Paper 1 (The Swedish Institute of International Affairs 2020).

57 W. Saad, M. Bennis & M. Chen, *A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems*, 34(3) IEEE Network 134–142 (May/June 2020).

58 5G PPP Security WG, *5G PPP Phase 1 Security Landscape*, white paper (2017); for a detail analysis of network security risks, *see* A. Ken Jakobsson & M. Stoltz, *Principled Big Tech: European Pursuit of Technological Autonomy*, in *Strategic Autonomy and the Transformation of the EU* (N. Helwig ed., The Finnish Institute of International Affairs 2021), https://www.fiia.fi/en/publication/strategic-autonomy-and-the-transformation-of-the-eu.

59 F. Yun Chee, *EU Demands Scrutiny of 5G Risks, But no Bloc-wide Huawei Ban* (Reuters 26 Mar. 2019).

60 A. Segal, *Huawei, 5G, and Weaponized Interdependence*, in *The Uses and Abuses of Weaponized Interdependence* 149–165 (D.W. Drezner, H. Farrell & A. Newman eds, Brookings Institution Press 2021).

61 L. Cerulus, *Huawei Challenges Legality of 5G Bans in Poland, Romania* (2 Nov. 2020), https://www.politico.eu/article/huawei-hints-at-legal-action-against-5g-bans-in-poland-romania/ (accessed 29 Nov. 2021).

62 The White House, *Executive Order on America's Supply Chains*, 24 Feb. 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/ (accessed 11 Aug. 2021).

also a significant increase in the reshoring of US manufacturing away from China and, more broadly, Asia.[63]

The EU Commission has communicated the cybersecurity of 5G networks to be 'an issue of strategic importance for the Union' and that ensuring 'European sovereignty should be a major objective'. [64] The Commission – similarly to the Strategic Outlook on China – recognizes that 'cybersecurity of 5G networks is key for ensuring the strategic autonomy of the Union'. Here cybersecurity could be understood as ensuring control over information flows. This means that for the 5G ecosystem's functioning, the EU cannot be dependent on a particular device or service supplier.

Besides the traditional technological security concerns of 5G, [65] it has captured the attention in the national security sphere.[66] Rühlig and Björk have analysed the 5G issue in Europe and Huawei's role in it. They divide 5G risks into *network security risks* and *technological dependency*, of which the latter is perhaps more significant, as Europe's technological dependence on China is already high.[67] EU Member States hold a variety of positions and perceptions on Chinese 5G technology. In 2019, dependence on Huawei-built infrastructure ranged from 80–90% in Belgium and Czech Republic, to 60% in Germany and Poland, some 50% in Denmark and 30% in France.[68] While Huawei is now effectively banned in some countries, such as in France since 2021, several Member States, such as Austria and Malta, have become dependent on Huawei as primary vendor.[69] However, current levels of actual technological dependency do not tell the full story. In the context of intensifying rivalry with China and increasing suspicions of China's motives, as important for risk assessment is the lack of trust in EU-China relations, and the *perceived* potential for China to be in a future position, where it could use 5G as a chokepoint in conflict situations.

The situation evolves constantly and requires the EU's legal system to take a stance on national security exceptions. On 20 October 2020 Sweden

---

63 Kearney, *Trade War Spurs Sharp Reversal in 2019 Reshoring Index, Foreshadowing COVID-19 Test of Supply Chain Resilience*, https://www.kearney.com/operations-performance-transformation/article?/a/trade-war-spurs-sharp-reversal-in-2019-reshoring-index-foreshadowing-covid-19-test-of-supply-chain-resilience (accessed 27 Aug. 2021).

64 *Commission Recommendation (EU) 2019/534 of 26 Mar. 2019 Cybersecurity of 5G Networks C/2019/2335*, OJ L 88, 42–47 (29 Mar. 2019).

65 Ahmad et al., *supra* n. 48.

66 K. Kaska, H. Beckvard & T. Minárik, *Huawei, 5G and China as a Security Threat*, CCDCOE Nato Cooperative Cyber Defence Centre of Excellence (Tallinn, 2019).

67 Rühlig & Björk, *supra* n. 56.

68 *Ibid*.

69 Hillman, *supra* n. 54, at 450.

announced that it will not allow Huawei or ZTE gear to be used by firms taking part in its 5G spectrum auction. The Chinese Foreign Ministry expressed its disapproval of Sweden's decision and urged Sweden to 'correct its mistake and to avoid [a] negative impact on the Swedish businesses operating in China'.[70] Swedish competing equipment provider Ericsson has publicly indicated concerns about losing market access in China because of retaliation.[71] In 2021, Huawei invoked EU freedoms when it tried to persuade the Administrative Court of Appeal in Stockholm to submit a preliminary ruling reference to the Court of Justice of the European Union (CJEU).[72] This case might become a precedent.[73] As a parallel legal process to the same 5G saga, on December 2020 Huawei submitted a notice of intent to launch an investment arbitration dispute against Sweden under the International Centre for Settlement of Investment Disputes (ICSID).[74] Huawei alleges a breach of the investment protection standards under the Sweden-China BIT,[75] amounting to hundreds of million euros.[76] In January 2022, Huawei initiated arbitral proceedings against Sweden.[77]

The current state of 5G in the context of EU's strategic autonomy illustrates that the EU's ability to manage its interdependencies is limited. Member States have great leeway to decide how to manage the build-up of 5G networks, and the Union is consequently divided in its approach to Huawei. The pressures coming from the US do not help in alleviating these internal divisions. While the potential decision from the CJEU is likely to bring some clarity to certain market access aspects of EU rules, the EU has also tried to change its reactive approach regarding 5G and tried to develop new tools, namely the 5G toolbox.

---

70 PRC Foreign Ministry, *Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference* (21 Oct. 2020), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1825675.shtml (accessed 11 Aug. 2021).

71 Financial Times, *Ericsson Warns of China Retaliation Following Sweden's Huawei Ban*, 16 July 2021, https://www.ft.com/content/2a596954-1206-4ce2-9dca-9c128d326768 (accessed 29 Nov. 2021).

72 Huawei, *Huawei Technologies komplettering av överklagandet av förvaltningsrättens dom avseende svenska 5G-licensvillkoren* (1 Oct. 2021), https://www.mynewsdesk.com/se/huawei-swe-corporate/pressreleases/huawei-technologies-komplettering-av-oeverklagandet-av-foervaltningsraettens-dom-avseende-svenska-5g-licensvillkoren-3132774 (accessed 29 Nov. 2021).

73 L. Cerulus, *Huawei Seeks EU Court Involvement in Swedish ban*, Politico (6 Oct. 2021), https://www.politico.eu/article/huawei-sweden-china-5g-court-case-european-union/ (accessed 29 Nov. 2021).

74 Huawei Technologies Co., Ltd. *v.* Kingdom of Sweden (ICSID Case No. ARB/22/2), Notice of Intent 31 Dec. 2020.

75 *Agreement on the Mutual Protection of Investments entered into Between the Kingdom of Sweden and the People's Republic of China on 29 Mar. 1982 as Amended on 27 Sept. 2004* ('Sweden-China BIT').

76 Huawei Technologies Co., *supra* n. 74.

77 Huawei Technologies Co., Ltd. *v.* Kingdom of Sweden (ICSID Case No. ARB/22/2).

5 THE EU'S ARSENAL OF COUNTERMEASURES: INVESTMENT SCREENING AND THE 5G TOOLBOX

The security threats posed for the Union are of both a conventional and a non-conventional nature.[78] In this article, the *investment screening* regulation[79] and the *5G toolbox*[80] are understood as coordinated countermeasures to level the playing field and tackle security threats to the autonomy of the Union's institutions and Member States in the maritime and information technology networks. Respectively, both port infrastructure and 5G are considered as hubs of critical networks for flows of goods and information.

The investment screening regulation originates in EU ambitions to protect business assets (that contribute to European strategic autonomy) from foreign investors that 'could threaten legitimate public policy objectives'.[81] The investment screening regulation is aimed at reinforcing the ability of Member States to screen foreign investment based on security and public order, as well as to enhance cooperation between the Commission and the Member States. The screening regulation also aims to harmonize the outline of national screening mechanisms if a particular Member State decides to implement such a mechanism. Importantly, the Commission has the possibility to issue only non-binding opinions pursuant to the regulation. The importance of direct investments as acquisitions – and governance of those in national security-related areas – comes with obtaining significant management influence, typically above 10% of voting rights. To align with the conceptual framework, the main function of the screening regulation is to enable advantageous information exchange about foreign investments. Additionally, if a Member State has implemented a domestic investment screening mechanism, to make it possible to deny (partly or wholly) an investment.

Although the European Commission has announced that the screening regulation does not target any specific country,[82] several writings have assigned

---

78 A. Suzana, B. Immenkamp, E. Lazarou, J. L. Saulnier & A. B. Wilson, *On the Path to 'Strategic Autonomy': The EU in an Evolving Geopolitical Environment*, 37 (Sept. 2020), https://europarl.europa.eu/RegData/etudes/STUD/2020/652096/EPRS_STU(2020)652096_EN.pdf (accessed 29 Nov. 2021).

79 *Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 Mar. 2019 Establishing a Framework for the Screening of Foreign Direct Investments Into the Union*, OJ L 79I, 1–14 (21 Mar. 2019).

80 NIS Cooperation Group, *Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures*, CG Publication 1 (2020).

81 European Council, *Joint Statement of the Members of the European Council*, Brussels (26 Mar. 2020), https://www.consilium.europa.eu/media/43076/26-vc-euco-statement-en.pdf (accessed 29 Nov. 2021).

82 European Commission, *Frequently Asked Questions on Regulation (EU) 2019/452 Establishing a Framework for the Screening of Foreign Direct Investments Into the Union*, https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157945.pdf (accessed 29 Nov. 2021).

Chinese FDI as a potential target.[83] In 5G, the EU's vaunted regulatory and standard-setting powers – or what Bradford calls 'the Brussels Effect'[84] – have been challenged, as China has increasingly placed itself at the centre of global standard-setting. The European Parliament, in its resolution of 12 March 2019 called on the Commission to develop a strategy that puts Europe in a leading position in cybersecurity technology and reduces dependency on foreign technology. The Parliament recognized that the Chinese technological presence in the EU poses a security threat and requires it to act at the Union level.[85] In response, the European Commission on 26 March 2019 adopted Recommendation (EU) 2019/534 on the cybersecurity of 5G networks.[86] Once active, 5G networks will form the backbone that will ensure the functioning of critical infrastructure and various systems, such as banking, health, energy, transport, and other industrial and other societal systems, including democratic elections.

These communications, the collection of national risk assessments on 9 October 2019[87] and conclusions made by the Council on 3 December 2019 [88] led to a publication of the *Cybersecurity of 5G networks – EU toolbox of risk mitigating measures* ('5G toolbox') by the Network and Information Systems (NIS) Cooperation Group in January 2020.[89] The 5G toolbox aims to avoid technological dependency on a potentially hostile extra-EU state actor, i.e., prevent it gaining chokepoint powers. The 5G toolbox does not establish a new framework of tools for mitigating those risks. Instead, it identifies a set of existing measures to mitigate the risks of 5G networks. Those existing measures include the telecommunication sector-specific legal tools, e.g., the EU telecommunication framework,[90] the NIS Directive (Directive on security of network and information

---

83 *See* e.g., MERICS Briefs, *China's New Export Control Law*, MERICS China Essentials (22 Oct. 2020), https://merics.org/en/briefing/chinas-new-export-control-law (accessed 29 Nov. 2021); L. Reins, *The European Union's Framework for FDI Screening: Towards an Ever More Growing Competence Over Energy Policy?,* 128 Energy Pol'y 665–672 (2019).

84 A. Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

85 European Parliament, *Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them*, 2019/2575, RSP (2019).

86 Commission Recommendation 2019/534, *supra* n. 64.

87 European Commission, *EU-Wide Coordinated Risk Assessment of 5G Networks Security*, Press release (9 Oct. 2019), https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security (accessed 29 Nov. 2021).

88 Council of the European Union, *Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G*, 14517/1 (3 Dec. 2019).

89 NIS Cooperation Group, *Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures*, CG Publication 1 (2020).

90 *Directive 2002/21/EC as Last Amended by Directive 2009/140/EC of 25 Nov. 2009 on a Common Regulatory Framework for Electronic Communications Networks and Services*, OJ L 337, 37–69 (18 Dec. 2009); and *Directive 2018/1972 of 11 Dec. 2018 Establishing the European Electronic Communications Code*, OJ L 321, 36–214 (17 Dec. 2018).

systems),[91] and the Cybersecurity Act,[92] as well as certain other relevant mechanisms, including the investment screening and trade defence instruments. The outcome of the 5G toolbox is that Member States should restrict the access of high-risk suppliers, maintain diverse 5G supply chains (including screening investments affecting key 5G assets), and strengthen the EU's 5G capabilities.[93] The aim is to maintain control over the EU's communication networks and recognize the possibility of prohibiting potential and harmful investments targeting EU 5G assets.

Investment screening systems also have a crucial importance in relation to the Union's 5G toolbox. The Commission has underlined that 'foreign investment in strategic sectors, acquisition of critical assets, technologies and infrastructure in the Union and supply of critical equipment may also pose risks to the Union's security'.[94] However, a fundamental difference is that the 5G toolbox resembles more of a coordinated action plan rather than a new instrument *per se*, as the investment screening regulation is. Nevertheless, both mechanisms, and their nature, touch on the fact that the EU has limited competence on issues related to Member States' national security. Despite the political will behind these motivations to enhance EU's strategic autonomy, there are de jure limitations to the EU's capacity to act.

The boundaries of the EU's competences are governed by the principle of conferral.[95] The EU may act only within the boundaries of the competences that have been conferred upon it by the Member States, viz. competences that are not conferred to the EU, remain with the Member States.[96] National security remains the sole responsibility of each Member State.[97]

The first part of the competence discussion around investments is relevant to understanding the nature of the screening regulation. The Treaty of Lisbon enlarged the powers of the EU vis-à-vis FDI (Articles 206 and 207 of the Treaty on the Functioning of the European Union 'TFEU'[98]), as part of the Common Commercial Policy, which is within the exclusive competence of the EU. FDI flows are generally

---

91 *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, OJ L 194, 1–30 (19 July 2016).

92 *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 Apr. 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, OJ L 151, 15–69 (7 June 2019).

93 5G toolbox, *supra* n. 80, at 18.

94 Commission Recommendation 2019/534, *supra* n. 64.

95 Treaty on European Union ('TEU', Consolidated version of the Treaty on European Union EUVL C 326, 26 Oct. 2012), Art. 5(1).

96 TEU Arts 4(1) & 5(2).

97 TEU Art. 4(2).

98 Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1.

capital movements. Although Member States are obliged to follow the TFEU Article 63 on the free movement of capital, viz. all restrictions on the movement of capital between Member States and between Member States and third countries shall be prohibited, TFEU Article 65 imposes exceptions to it. Pursuant to Article 65, the free movement of capital is without prejudice to the right of Member States to take measures which are justified on the grounds of public policy or public security. In 2000, the CJEU confirmed that public policy or public security are valid excuses to prevent adverse investments.[99] However, public security-based measures need to be proportional and necessary.[100] Article 346 of the TFEU has also been used to enable Member States to protect their national security interests.

Although the Commission considered as a mere option the provision 'to propose an FDI screening mechanism entirely operated at EU level', it was regarded to be not only 'very difficult to operate in practice due to the possible differences of views amongst Member States', but also 'due to the fact that national security remains the sole responsibility of Member States'.[101] Clearly, the Commission acknowledged that there was not a high likelihood of winning approval for an EU-wide screening mechanism. However, the Commission seems to be looking ahead and ready to enhance the existing mechanism.[102]

While the European Commission calls for the 'full use of the existing EU tools and instruments',[103] through the screening of potential FDI to key 5G assets, the issue of the effectiveness of the investment screening regulation becomes relevant. First, it is necessary to underline that the investment screening regulation in its current form is merely a cooperation and information exchange tool. The final word still resides with Member States. In case of significant economic interest, a hypothetical EU Member State might shift the balance more towards a 'risky' 5G infrastructure. Yet, it would not be a huge surprise after Member States have adopted an EU-standard for a national screening mechanism, to increase European integration in this field later, when there is enough political momentum for it.

The second part of the competence discussion revolves around the traditional legal instruments contained in the 5G toolbox, namely the *EU telecommunication framework* as a common regulatory framework for electronic communications

---

99 Case C-54/99 *Association Église de Scientologie de Paris, Scientology International Reserves Trust and the Prime Minister* [2000] ECLI:EU:C:2000:124, para. 20.

100 *See* Case C-423/98 Alfredo Albore [2000] ECLI:EU:C:2000:401.

101 European Commission, *Accompanying the document Proposal for a Regulation of the European Parliament and of the Council Establishing a Framework for Screening of Foreign Direct Investments Into the European Union* (2017) Staff working document, SWD/2017/0297 final - 2017/0224 (COD).

102 European Commission, *supra* n. 22.

103 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Secure 5G deployment in the EU - Implementing the EU toolbox*, COM(2020) 50 final, 6 (Brussels, 29 Jan. 2020).

networks and services, and the *NIS Directive* as a cyber security tool to enhance cooperation among the Member States and preparedness to security threats in critical sectors, such as transport and digital infrastructure. Here, the instruments are directives that are tools for harmonization and approximation of national laws. The Communication on the implementation of the NIS Directive by the Member States shows that it was a matter of concern to the Commission.[104] Also, the NIS Directive comes close to the national security of Member States. Thus, it was made clear that the directive applies without prejudice to Article 346 of the TFEU, which provides that Member States are not obliged to supply information, the disclosure of which it considers contrary to its' essential security interests.

6 DE-WEAPONIZING CRITICAL HUBS?

We have explored EU efforts to obtain strategic autonomy by focusing on two critical sectors: port infrastructure and 5G, identifying them as critical chokepoints with strategic importance for the Union in its attempt to reach strategic autonomy. Both sectors have a 'connectivity' function and can be regarded as critical hubs. Our analysis of the EU's countermeasures demonstrates that the EU has strived to 'de-weaponize' these critical hubs, i.e., prevent their being exploited by a future adversary.

Our findings suggest the existence of the theoretical possibility of foreign (economic) coercion in both cases, taking advantage of chokepoint effects. Since the EU does not have exclusive authority over those hubs, due to national security competence limitations, it cannot effectively control them in the interest of the Union. The screening regulation and the 5G toolbox rely on the 'sincere cooperation' between the EU institutions and the Member States, meaning that Member States and the EU shall assist each other in carrying out tasks deriving from the EU treaties and requiring Member States to facilitate to the achievement of the EU's tasks, and to 'refrain from any measure which would jeopardize the attainment of the Union's objectives' (TEU Article 4(3)). One of the fundamental questions is, can the EU be resilient against coercive inward investment if it does not possess effective enforcement mechanisms to intervene in critical infrastructure investments at the national level? Are the soft mechanisms currently in place enough to achieve the EU's strategic autonomy goals?

Our analysis concludes that the quest to attain the political goal of a higher degree of strategic autonomy for the EU vis-à-vis external actors is still hampered

[104] European Commission, *Communication from the Commission to the European Parliament and the Council: Making the most of NIS – Towards the Effective Implementation of Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, COM (2017) 476 final/2 (Brussels, 4 Oct. 2017).

by the competence limitations of the Union to act in critical areas. Much of the heavy lifting in implementing EU policy goals falls on Members States with varied economic and security interests. As the EU's official policy stance on China is a mixture of partnership, competition, and rivalry, it is scarcely surprising that Member States put different weights on these three components.

It should, however, be noted that it is somewhat irrelevant whether Chinese ownership and involvement in critical hubs constitutes a *real* threat. Perceptions of China have, for better or worse, changed in Europe over the past few years, ushering in what has been described as a *Gestalt shift*.[105] Both the EU collectively, and many Member States individually, act *as if* Chinese ownership of critical infrastructure assets is inherently more threatening than, say, similar Canadian investments would be. This resembles the classical case in international relations, where it matters greatly *who* does something for *how* those actions are perceived. For example, nuclear weapons possessed by North Korea are inherently more threatening to the United States than nuclear weapons possessed by the United Kingdom.[106] Similarly, Chinese investments in EU critical infrastructure are now perceived as inherently more threatening than similar Canadian investments would be.

[105] M. Mattlin, *Kanariefågeln som tystnade. Finlands gestalt shift om kinesiska investeringar*, 78(1) Internasjonal Politikk 54–67 (2020).

[106] R. Jervis, P*erception and Misperception in International Politics* Princeton (Princeton University Press 1976).