European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2024)0028

Security and defence implications of China's influence on critical infrastructure in the European Union

European Parliament resolution of 17 January 2024 on the security and defence implications of China's influence on critical infrastructure in the European Union (2023/2072(INI))

The European Parliament,

– having regard to the Treaty on the Functioning of the European Union,

– having regard to Title V of the Treaty on European Union, in particular Chapter Two, Section Two thereof on provisions on the common security and defence policy,

– having regard to the 'Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security', approved by the Council on 21 March 2022 and endorsed by the European Council on 25 March 2022,

– having regard to the Versailles Declaration, adopted at the informal meeting of the Heads of State or Government on 11 March 2022,

– having regard the joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 20 June 2023 on European economic security strategy (JOIN(2023)0020),

– having regard to the Regulation (EU) 2022/2560 of the European Parliament and of the Council of 14 December 2022 on foreign subsidies distorting the internal market[1],

– having regard to 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[2],

– having regard to 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 (Resilience of Critical Entities Directive)[3],

---

1 OJ L 330, 23.12.2022, p. 1.
2 OJ L 79 I, 21.3.2019, p. 1.
3 OJ L 333, 27.12.2022, p. 164.

– having regard to 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)[1],

– having regard to the Commission proposal of 15 September 2022 for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454),

– having regard to Regulation (EU) 2023/1781 of 13 September 2023 of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)[2],

– having regard to its position in first reading on a proposal for a Regulation of the European Parliament and of the Council establishing a framework for ensuring a secure and sustainable supply of critical raw materials (Critical Raw Materials Act) in the TA adopted with the non-finalised version[3],

– having regard to Regulation (EU) 2023/2675 of 22 November 2023 of the European Parliament and of the Council establishing the protection of the Union and its Member States from economic coercion by third countries[4],

– having regard to its resolution of 16 September 2021 on a new EU-China strategy (2021/2037(INI))[5], inter alia aimed at strengthening the EU's 'trade toolbox' to help mitigate the current imbalance in bilateral economic and trade relations between China and the EU,

– having regard to Parliament's resolutions of 9 March 2022[6] and of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation[7],

– having regard to the joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank of 1 December 2021 entitled 'The Global Gateway' (JOIN(2021)0030),

– having regard to the Commission recommendation of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States (C(2023)6689),

---

1 OJ L 333, 27.12.2022, p. 80.
2 OJ L 229, 18.9.2023, p. 1.
3 Proposal for a Regulation establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) 168/2013, (EU) 2018/858, 2018/1724 and (EU) 2019/1020 (COM(2023)0160).
4 Proposal for a Regulation on the protection of the Union and its Member States from economic coercion by third countries (COM(2021)0775) (OJ L, 2023/2675, 7.12.2023).
5 OJ C 117, 11.3.2022, p. 40.
6 Texts adopted, P9_TA(2023)0219.
7 Texts adopted, P9_TA(2023)0219.

– having regard to the Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure[1],

– having regard to the Vilnius Summit Communiqué, issued by the NATO heads of state and government participating in the meeting of the North Atlantic Council in Vilnius on 11 July 2023,

– having regard to the Final Assessment Report of the NATO-EU Task Force of 29 June 2023 on the Resilience of Critical Infrastructure,

– having regard to the Joint Declaration of 10 January 2023 on EU-NATO Cooperation,

– having regard to the G7 Hiroshima Leaders' Communiqué of 20 May 2023,

– having regard to the Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan of 24 October 2023,

– having regard to Rule 54 of its Rules of Procedure,

– having regard to the opinion of the Committee on International Trade,

– having regard to the report of the Committee on Foreign Affairs (A9-0401/2023),

A. whereas the recent joint communication on a European economic security strategy focuses on minimising and managing the risks arising from certain economic flows and the EU's dependency on authoritarian and totalitarian regimes such as the People's Republic of China (PRC) in the context of increased geopolitical tensions and accelerating technological shifts, while protecting free market principles from distortion by such regimes and, thereby, preserving maximum economic openness and dynamism;

B. whereas disruptions to critical infrastructure can have significant negative consequences for vital government functions, essential services for the population, economic activity as well as the security and defence of the EU; whereas it is crucial that Member States and the Commission be vigilant with regard to financial investments that foreign countries make in the operation of critical entities within the EU and the consequences that such investments could have on the ability to prevent significant disruptions;

C. whereas the Resilience of Critical Entities Directive[2] and the NIS 2 Directive[3] provide a comprehensive legal framework to strengthen both the physical and digital resilience of critical infrastructure, including that related to energy, transport, health, digital infrastructure, water and food;

D. whereas since the Council Recommendation of 8 December 2022 was issued, targeted actions have already been carried out to ensure a common EU response to incidents,

---

1 OJ C 20, 20.1.2023, p. 1.

2 Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164).

3 Directive (EU) 2022/2555 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) (OJ L 333, 27.12.2022, p. 80).

including by strengthening coordination with NATO through the EU-NATO Task Force on the resilience of critical infrastructure embedded in the NATO-EU Structured Dialogue on Resilience;

E. whereas European ports in which Chinese state-owned companies have stakes handle more than 10 % of Europe's total shipping container capacity; whereas 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, greatly increasing the risk of espionage;

F. whereas the coercive policies and the growing assertiveness of the People's Republic of China (PRC), including its increasingly aggressive stance towards Taiwan and the aggressive posture assumed in the South China Sea, as well as the social and economic consequences of the COVID-19 pandemic and the Russian war of aggression against Ukraine have exposed the EU's vulnerabilities and reaffirmed the need to 'de-risk' its relations vis-à-vis the PRC and other undemocratic third countries;

G. whereas the Chinese government has demonstrated that it is willing to weaponise its overwhelming control of global rare earth supplies for political ends and to obtain unfair economic concessions and advantages;

H. whereas China is restricting non-Chinese companies from participating in infrastructure projects on account of the security risks and is putting forward legislation with regard to critical infrastructure, such as the Critical Information Infrastructure Security Protection Regulations; whereas China is involved in constructing EU-funded infrastructure in various EU Member States; whereas pursuant to international commitments, it is possible for the EU and the Member States to adopt restrictive measures relating to foreign direct investment (FDI) on the grounds of security or public order, subject to certain requirements; whereas in 2021-22, China engaged in an economic blockade against Lithuania in response to Lithuania's decision to withdraw from the Belt and Road Initiative and to open a Taiwanese Representative Office in Lithuania, resulting in the Commission's request to establish a panel at the World Trade Organisation to examine the legality of China's trade restrictions against Lithuanian and EU exports containing Lithuanian content, and whereas this demonstrates China's assertiveness in targeting specific EU countries, not only through direct economic coercion, but also through the threat of secondary sanctions;

I. whereas the spread of China's digital authoritarianism and mass surveillance continues to intensify both within China and beyond, targeting democratic institutions and societies, and it risks establishing a new international order that would endanger freedom and democracy around the world; whereas a large number of Chinese students study in Member States' universities, especially in the field of dual-use technologies, potentially leading in some cases to a high risk of espionage; whereas former European fighter pilots have been employed by the Chinese army and such recruitment creates a serious risk of transfer of critical information putting the military-strategic interests of the countries concerned at risk; whereas Chinese ambitions are growing in strategic areas such as AI, cloud computing, semiconductors, or hardware; whereas these instruments, particularly AI, could be developed for military purposes, driving the next revolution in military affairs;

J. whereas China's acquisition of critical infrastructure, especially within the EU and in its neighbourhood, including the Western Balkans and Africa poses an increasing multi-dimensional risk to the EU's security;

K. whereas China's national security related legislation, such as the 2015 National Security Law of the People's Republic of China, requires citizens and organisations to provide support and assistance to the PRC's public security, state security or military bodies;

L. whereas the Sino-Russian strategic partnership formalised with the Joint Statement 'on the international relations entering a new era and the global sustainable development' of 4 February 2022 continues to grow, including in the areas of technology and military know-how and capability transfers, posing an increasing threat to European security;

The core of the problem: understanding China's military-civil fusion strategy

1. Underlines that China's military-civil fusion (MCF) strategy is a state-led, state-directed programme and plans to instrumentalise all levers of state and commercial power to strengthen and support the Chinese Communist Party (CCP) and its armed wing, the People's Liberation Army (PLA), particularly by acquiring and diverting the world's cutting-edge technologies, with the objective of strengthening the totalitarian regime and achieving military dominance;

2. Considers that China's party-driven political system and economy often require private companies to align their commercial interests with the CCP, including its military activities, repression, influence and political interference activities; notes that CCP party cells inside private companies are commonly used as tools of direct party control; highlights that, consequentially, Chinese companies' international activities support the CCP's goals of expanding its influence in third countries, undermining geopolitical rivals and increasing China's influence;

3. Believes that MCF must be understood in a larger geopolitical, economic and strategic context, taking into account its interconnections with other initiatives, such as the Belt and Road Initiative, the Digital Silk Road (including Made in China 2025, China Standards 2035), the Global Security Initiative, Dual Circulation strategy) and China's increasing assertiveness and aggressive posturing abroad; believes that the ultimate aim of MCF is to advance the party-state's long-term strategic goal to become the world's leading power in terms of political influence, economic capacities, technological dominance and military might, and to undermine the rules-based international order;

4. Recalls that achieving primacy in science and technology has been one of the CCP's top priorities in recent years and that the CCP's MCF strategy incentivises the sharing of research and development results between market-oriented and Chinese defence industries; stresses the repeated warnings by intelligence agencies against the risks of economic dependence, espionage and sabotage caused by the economic presence of entities from certain non-EU countries, in particular China, in critical infrastructure and strategic sectors across the EU; is, in this regard, concerned by the political pressure asserted in the approval of specific Chinese investments into critical infrastructure, as in the case of the German government's decision to agree to the acquisition of a stake at the port of Hamburg by COSCO, contrary to the advice of the competent institutions;

Consequences of the PRC's military-civil fusion strategy

5. Warns of the risk of Chinese companies having any involvement with EU strategic assets, especially those companies that have direct or indirect links to China's political-military or intelligence systems; underlines, in this regard, its concern that technology and technological expertise used in civilian activities, particularly in the economic sphere, continues to be transferred to China's military, increasing the PLA's ability to develop the next generation of military technology, which may be used to coerce partners in Asia and around the world; urges EU Member States to increase regulatory oversight and introduce specific background checks over individuals and legal entities with direct ties to the Chinese government;

6. Is concerned that that 98 % of EU demand for rare earths is being met by the PRC; emphasises that China produces 70 % of the world's batteries (hosting three of the top five battery manufacturing giants), accounts for 60 % of global aluminium production and 75 % of silicon production, as well as 94 % the global production of gallium and around 60 % of germanium production, and is the leading refiner of 60 % of lithium and 70 % of copper processing and produces 84 % of the world's nickel and 85 % of its cobalt; underlines that Chinese mining companies are active in Serbia (copper and gold), the Democratic Republic of Congo (cobalt), Indonesia (nickel) and Chile and Australia (lithium) and that its quasi-monopoly in the production and processing of these critical commodities creates crucial dependencies and therefore presents not only an acute geopolitical challenge for the EU, but also a huge risk for Europe's defence and other key industrial sectors as well as its open strategic autonomy and European economic security strategy;

7. Welcomes, in this regard the Commission proposal for the Critical Raw Materials Act and calls for the speedy implementation of its goals in order to strengthen the EU's supply chain resilience; recalls that critical raw materials are essential to the security and defence sector as well as for the success of the EU's digital and green transitions; calls on the Commission and the Member States, in coordination with industry stakeholders to implement the decision to gradually reduce the dependence on China by diversifying the sources of critical raw minerals and rare earth elements, establishing strategic partnerships with reliable third countries with a view to ensuring a secure and reliable supply of critical raw materials; urges the EU to assist Member States in developing projects that will aim for greater independence from Chinese production;

8. Strongly advocates for the diversification of suppliers and partners in critical infrastructure initiatives to reduce the vulnerability to external influences, ensuring that reliance on any single source is minimised;

9. Is concerned that privately owned undersea cables provided by Chinese companies, such as HMN Technologies, a PLA cyber intelligence–affiliated entity, are used to support EU and Member States' diplomatic and military communications; expresses its grave concern over the undersea data cable systems operated by Chinese company HMN Technologies, which connect EU Member States' territories and the Indo-Pacific region, including Member State and NATO military bases, creating security vulnerabilities as regards cybersecurity, underwater surveillance, data collection, and gathering of intelligence; in this regard, is further concerned by the sale of a Dutch company, the backbone of Estonia's internet infrastructure, to a Chinese company linked to the PLA; highlights the need for a joint effort among the Member States to prevent similar cases;

10. Recalls the need to perform a thorough evaluation of the EU institutions' information security infrastructure and services, in particular regarding classified communications between the institutions and missions and operations abroad; recalls that the full supply chain should be taken into account to ensure that the companies do not have any direct or indirect links with the PRC; calls for specific provisions in EU institutions procurements procedures to limit the risk of interference, including the acquisition, maintenance or vetting by a third party;

11. Warns that major investments in seaports, railways and airports give Beijing the opportunity to monitor and control activities in key logistical nodes with a fundamental strategic dimension;

12. Highlights the fact that, in 2022, China was the EU's second largest trading partner for goods; expresses concern about the increasingly imbalanced trade and investment relationship between the EU and China, which is also highlighted by the EU's record trade deficit of EUR 396 billion in 2022 and its dependence on Chinese imports and investments in some critical sectors; highlights China's imbalanced international trade policy in the context of its dual circulation strategy; asks the Commission to raise the EU's concerns with China on its managed trade practices;

Developing responses: expanding the toolkit to respond to security and defence concerns

13. Argues that a key area of EU critical infrastructure is its network of research institutes and research and development facilities, which play an important role in the EU's ability to deliver on its green and digital transition commitments, alongside key arenas such as space defence; recalls the security vulnerabilities linked to forced technology transfers, intellectual property theft and knowledge leaks, both in the EU and abroad; calls for increased vigilance when accounting for such threats to the EU's ability to innovate and foster growth;

14. Notes that Chinese companies are already leaders in key technologies used in sectors such as 5G wireless infrastructure, drones, batteries, hypersonic missiles, solar and wind energy, as well as cryptocurrency; expresses its concerns over the uses of these technologies and the dependencies they create; notes, in this regard, that 100 % of the 5G RAN in Cyprus is composed of Chinese equipment, and 59 % in the case of Germany; stresses that this runs counter to the EU's '5G security toolbox' guidelines to mitigate security risks in networks and calls on the Council and the Commission to exclude the use of equipment and software from manufacturers based in the PRC in core network functions; recalls that Huawei has been participating in 11 projects under Horizon Europe until June 2023, thus receiving EUR 3,89 million of funding in total; therefore, urges the EU and European institutions to carry out a systematic screening of Chinese companies benefiting directly or indirectly from European programmes of strategic importance for the EU and, where necessary, terminate their participation; furthermore, calls on the Commission to propose additional security standards for Chinese suppliers of 5G and the next generation 6G network;

15. Considers the TikTok app, owned by Chinese conglomerate ByteDance, to be in breach of the European data privacy framework, making it a potential risk and a source of Chinese-backed disinformation; welcomes the decision of EU institutions and those of several EU Member States to suspend the use of the TikTok application on corporate devices, as well as personal devices enrolled in the institutions' mobile device services;

16. Warns that the deterioration in the security environment in Europe, in its neighbourhood, and around the globe requires urgent reflection on how to strengthen the EU's open strategic autonomy and reduce its dependence on countries such as the PRC and systemic rivals that pose a security threat to the EU; stresses the need to prevent sensitive emerging technologies and key dual-use items, especially those that are critical to the EU's security and defence from being transferred to destinations of concern that pursue or collaborate in MCF strategies; regards the establishment of EU-wide electronic customs and export licensing systems to be a critical step towards effective common European export controls and urges all Member States to make these systems operational by the end of 2024; furthermore calls on the EU institutions and the Member States to strengthen cooperation with the transatlantic and other like-minded partners in the protection of critical infrastructure, and to defend democracy and preserve our shared values, security and prosperity;

17. Remains concerned that European critical infrastructure, from telecommunications networks to port facilities, is becoming increasingly vulnerable to external influence; commends, in this regard, recent legislative steps to enhance the resilience of critical entities in the EU; notes with concern, however, that such initiatives are largely limited to FDI screening procedures, leaving other channels open for the CCP to gain access to and influence over critical assets, including through elite capture, technology and intellectual property transfers, as well as supply chain and sales market dependencies; notes that the establishment of a thorough risk assessment and mapping framework is imperative to identifying critical infrastructure assets and their susceptibilities; considers it necessary to map, track and assess China's and other third countries' access to critical infrastructure in the EU and to jointly proceed with mitigating measures where necessary; in this regard, calls on the Commission, with the support of the Member States, to compile an exhaustive inventory of critical assets and systematically evaluate their vulnerability to external influences; and therefore calls for the expansion of the legislative initiatives to address such risks;

18. Calls on the Commission to share with Parliament, before the end of this parliamentary term, a detailed analysis of the trade risks linked to technologies such as semiconductors, quantum computing, block chains, space, artificial intelligence and biotechnologies and the possible need for EU action in these fields;

19. Recalls that the FDI screening regulation[1] addresses risks to security and public order resulting from investments from outside the EU; notes the key added value of the screening mechanism as a pertinent tool that gives the EU and the Member States a better strategic overview and situational awareness of the trends, targets, means and methods deployed by foreign actors to increase their economic and political influence; calls for the current instruments that address FDI and foreign subsidies to be expanded to include generalised screening procedures for all stakeholders involved in EU critical infrastructure projects encompassing all modes of participation in critical infrastructure endeavours, including collaborative ventures, partnerships and technology transfers; also underlines that routine evaluations of critical infrastructure projects that involve non-EU stakeholders are essential and believes that this process should encompass scrutiny of ownership structures, dependencies within supply chains, and the transfer of technology associated with these projects; also, considers it necessary to establish due-

[1] Regulation (EU) 2019/452 of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 79 I, 21.3.2019, p. 1).

diligence standards to identify China's leverage over investors in EU critical infrastructure, and underlines that this approach should apply equally to candidate and potential candidate countries; stresses that the Member States are ultimately responsible for infrastructure protection, but have not consistently implemented current guidelines on FDI; is greatly concerned, in this regard, by the fact that not all Member States have in place or use mechanisms for screening foreign investment in critical infrastructure; urgently calls on the Member States to consistently implement current legislation related to FDI and on the resilience of critical entities;

20. Regrets in this regard the lack of adequate screening of risks of interference in public procurement related to security equipment, such as the case of the contract signed by Strasbourg airport to install airport security scanners and gates supplied by the European subsidiary of the Chinese company Nuctech, partly owned by the Chinese government and bound by the 'United Front' policy; warns that any such technologies could incorporate in-built security gaps or be accessed during their maintenance; on the other hand, welcomes the decision of the Romanian government to terminate negotiations with China General Nuclear Power Corporation, CGNPC, on the construction of nuclear reactors 3 and 4 at Cernavoda;

21. Stresses, however, that a strategic balance must be found between, on the one hand, the openness of the EU single market and its attractiveness for investments, and, on the other, the defence of the EU's critical infrastructure and autonomy, considering the EU's security vulnerabilities, especially as regards economic coercion or threats to the integrity of the EU's critical infrastructure;

22. Calls on the Commission to consider ways of making its opinions on FDI screening more impactful, in order to avoid distortions of the single market and a race to the bottom among Member States; calls on the Commission and the Member States to increase harmonisation, including by building appropriate expertise, and to fully implement the FDI screening regulation; believes that there is scope and the need for the regulation to be strengthened in its upcoming review at the end of the year; encourages the Commission to present an ambitious legislative proposal on a revised regulation addressing all the loopholes that have emerged during its implementation, and to swiftly evaluate the possibility of a legislative proposal on a screening mechanism for outbound investments; recommends building any proposed outbound investment screening mechanism on an impact assessment that includes appropriate consultation with businesses to minimise any potential negative consequences for European competitiveness;

23. Welcomes the new 'de-risking' approach in the proposed European economic security strategy of 20 June 2023, which aims to maximise the benefits of the EU's economic openness and to protect, promote and strengthen the EU's open strategic autonomy, while minimising the risks resulting from economic dependencies and their possible weaponisation, including investments and research collaboration in key enabling technologies with military applications, inter alia, in the areas of quantum computing, advanced semiconductors and artificial intelligence; calls for the swift adoption of the High Representative's and the Commission's proposals and calls on Member States to fully implement the EU's expanded regulatory framework to exclude entities that could contribute to MCF and to find alternatives for Chinese-financed projects in the EU through the development of a comprehensive approach to commonly identifying, assessing and managing risks to European economic security;

24. Further welcomes the High Representative and Commission's proposal to prevent the leakage of sensitive emerging technologies by establishing a list of dual-use technologies, based on narrowly defined and forward-looking criteria, such as the potential enabling and transformative nature of a technology, the risk of MCF and the risk of the technology being misused to violate human rights; calls on the Commission and the Member States to identify and implement the relevant protection measures for these dual-use technologies as soon as possible;

25. Calls, in this regard, on the Commission, in coordination with the Member States, to design a rapid response mechanism for the detection of the dual use, or misuse, of infrastructures in the EU under Chinese ownership, participation or concession, that could be used to terminate the rights of concession and/or suspend the capacity of domain in the cases of ownership and participation; calls on the Commission to annually report to Parliament on:

    (a) the detection of the possible dual use of strategic infrastructure that provides logistical and intelligence support to China;

    (b) the full respect of EU trade legislation, especially concerning due diligence, anti-coercion and goods made with forced labour entering the EU market;

26. Welcomes the adoption of the European Chips Act, which will increase the EU's ability to produce semiconductors and create a strategic map of, inter alia, capability gaps in the semiconductor value chain in the EU, thereby limiting the EU's dependence on third countries such as China; calls for further proposals to secure the production and supply chains of critical infrastructure and materials within the EU; further calls on the Commission and Member States to develop additional initiatives aimed at enabling closer coordination and collaboration with like-minded partners and allies, and to monitor and further develop, where possible and in line with the EU's aim to reduce further dependencies, global production capacities and supply chains in critical infrastructure and materials that are crucial to the security and defence of the EU; draws particular attention to Taiwan, which plays a significant role in the global supply chains and in the international rules-based order; reiterates its long-standing support for the EU-Taiwan Bilateral Investment Agreement and any arrangements mutually beneficial to bilateral trade and investment;

27. Calls on the Commission to propose a new legislative framework to mitigate the security risks coming from the suppliers of undersea cable systems, including through stricter monitoring and frequent review of the ownership structures of such suppliers, their previous investments in undersea cable systems and the proximity of the undersea cable systems to European and allied military bases; stresses the need to prevent cable system suppliers, such as Chinese companies, from sharing data with intelligence services other than to protect the infrastructure from outside intrusions or malign attacks; calls in this regard for initiatives aimed at the further development of European owned or based companies in the field of undersea cable systems;

28. Underlines that EU responses must be built around an augmented understanding of the relevant strategic picture centred on cross-policy and cross-national threat assessments and vulnerability studies on critical infrastructure; is of the opinion that a decentralised or neglectful approach, lacking clear visibility and scrutiny over projects with strategic significance for Europe's defence and security, could greatly harm the EU's geopolitical

interests[1]; recalls vulnerabilities linked to foreign interference, specifically in the information space, and the interplay between FDI projects and information manipulation operations by malign foreign actors;

Internal-external nexus: strengthening the resilience of the EU's closest partners

29. Expresses concern regarding the PRC's penetration of the EU market and its wider neighbourhood; calls on the Commission and the European External Action Service (EEAS) to ensure that the measures taken to strengthen the resilience of the EU in the face of Chinese influence, including de-risking, diversification and reduction of critical dependencies, are also extended to the EU's closest partners, in particular accession countries and those part of the EUs neighbourhood policy;

30. Recalls that the PRC's naval forces have means and legal tools to ensure that China's civilian ships and infrastructure can be used for military and security purposes; considers that China is able to use its civilian commercial infrastructure to support the PLA's presence in third countries; warns that such MCF provides the PLA with access to foreign ports, enabling it to pre-position logistics support to sustain naval deployments as far afield as the Indian Ocean, the Mediterranean Sea and the Atlantic Ocean; underlines that the risks of espionage are highest when Chinese civilian commercial assets are located in logistical hubs close to EU and NATO naval bases or port operators that have signed agreements to provide logistical support to European companies; calls on the Member States to urgently address the need to reduce the risks of espionage and sabotage in critical infrastructure, in particular those with a military function, such as ports that are used by NATO; stresses, in this regard, that the EU and NATO must work together to develop a long-term plan to counter China's MCF strategy in Europe and calls on the full implementation of the final assessment report of the EU-NATO task force[2];

31. Notes that ports are gateways to the world and as such play a crucial role in the EU's economy; notes with concern that Chinese-owned or controlled entities have strategically increased their stakes in European ports and port infrastructure; calls on the Commission to present an EU strategic policy framework to reduce and limit influence and operational control by China and other regimes; recalls also that PRC projects power overseas by using a network of commercial ports and dual-use facilities that provide logistics and intelligence support to the Chinese navy; notes that in 2022, Chinese companies owned or operated terminals in 96 ports across 53 countries; further notes that in at least nine ports, two of which are in Europe, People's Liberation Army Navy (PLAN) warships have undergone significant repairs or maintenance for vessels and equipment; points out that naval visits reveal areas of influence, prioritised operational zones, intelligence collection objectives and cooperation priorities;

32. Emphasises the need for a geopolitical approach to global cooperation on critical infrastructure in order for the EU to successfully face up to the new security challenges; notes that one third of all African infrastructure built since 2010, including around 50 %

---

1 Policy Department for External Relations of the Directorate-General for External Policies of the Union, 'Security implications of China-owned critical infrastructure in the European Union', June 2023.

2 European Commission, EU-NATO Task Force on the resilience of critical infrastructure: Final assessment report, June 2023.

of Africa's 3G networks and 70 % of its 4G networks, has been financed and constructed by Chinese state-owned enterprises; underlines that, over the past 20 years, China has increased its trade, investment and loan commitments by USD 160 billion with African Governments and their state-owned enterprises with few, or opaque, contractual obligations, predominantly in transportation, power generation, mining and telecommunications; highlights in particular the fact that a single Chinese telecommunication company has constructed up to 70 % of Africa's information technology infrastructure, as well as the role played by Chinese companies in the financing, building, expansion and renovation of at least 14 sensitive intra-governmental African telecommunication networks; expresses concern that the Chinese model is clearly attractive to many countries that cannot or are unwilling to satisfy EU requirements for access to equivalent levels of finance, thereby expanding Chinese influence to the detriment of EU partnerships and triggering risks of unsustainable debt for these countries, harming their long-term development to the detriment of their local population; calls on the Commission, the EEAS and Member States to intensify efforts, including attracting investments from the private sector, to implement the Global Gateway Investment Package of EUR 150 billion, agreed at the 6th EU-AU Summit in February 2022; urges the Council and the Commission to swiftly implement projects, especially lighthouse projects, under the initiative;

33. Underlines its concern that the PRC's strategy to build a 'blue economy cooperation base' along the coast of Africa, including through the construction of fishing vessels and vessel repairs facilities, could also be used for military purposes; stresses that there is a general lack of detail and transparency regarding these agreements and licences with African countries; outlines the potential geopolitical consequences for the EU, especially in third countries where the EU is engaged;

°

° °

34. Instructs its President to forward this resolution to the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, the Council and the Commission.