sipri

SIPRI Insights on Peace and Security

No. 2020/3 February 2020

EU SECURITY PERSPECTIVES IN AN ERA OF CONNECTIVITY: IMPLICATIONS FOR RELATIONS WITH CHINA

IAN ANTHONY, JIAYI ZHOU AND FEI SU

SUMMARY

● This SIPRI Insights Paper assesses European Union security perspectives on connectivity, alongside and in relation to the EU's evolving relationship with China. The EU's relations with China have undergone an important shift in recent years, with a strengthened emphasis by the EU on the challenges to bilateral cooperation. In addition, since 2014, EU and EU member states' security perspectives have undergone a wider reassessment—one that has increased the prominence of the military dimensions of connectivity, including military mobility, in EU security planning. The EU and China are currently pursuing synergies between their separate connectivity initiatives, namely the Belt and Road Initiative (BRI) and the Connecting Europe programme. However, there remain barriers to sustainable cooperation that will need to be addressed between them moving forward. This SIPRI Insights Paper outlines a number of those security concerns from the EU perspective, within the transport and digital sectors specifically.

I. Introduction

An important shift in the relations between the European Union (EU) and China is underway. The strengthening rhetoric from EU member states shows the growing concern over China's expanding economic presence and potential political influence in Europe; as a result, the EU has started to re-evaluate its policies towards China and reconfigure the relations between the two sides. This is evidenced in 'EU–China: A Strategic Outlook', a report published by the European Commission in March 2019, which recognizes China not only as a cooperation and negotiating partner, but also an economic competitor and systemic rival.[1] China's Belt and Road Initiative (BRI) has contributed to the evolution in EU–China relations, and it is now being examined in Europe as part of the overall assessment of relations with China.[2] Uncertainties stemming from United States–China tensions on nearly every front, including trade and technology, have also likely contributed.

In addition, the EU has suffered a major strategic shock: the annexation of Crimea by Russia in 2014 was the catalyst for a large-scale review of security requirements in Europe. One outcome of that review has been increased attention to military and non-military security, which are increasingly interconnected and have relevance to the growing connectivity between the EU and China.

Connectivity covers a spectrum of issues, including the improvement of the hard infrastructure of ports, railways, roads and pipelines, and soft infrastructure through trade, financial cooperation and people-to-people exchanges. This SIPRI Insights focuses on transport and digital connectivity. Digital and transport infrastructure are highly relevant to the plans that European countries are making in response to the new security environment in which they find themselves. Infrastructure is a potential target for a possible adversary because modern society is heavily dependent on the transport of people and goods and digital services. Infrastructure is

[1] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'EU–China: A strategic outlook', Joint communication to the European Parliament, the European Council and the Council, JOIN(2019) 5 final, Strasbourg, 12 Mar. 2019.

[2] For information about the BRI and implications for the EU, see Ghiasy, R. and Zhou, J., 'The Silk Road Economic Belt: Considering security implications and EU–China cooperation prospects', SIPRI, Feb. 2017; and Ghiasy, R., Fei, S. and Saalman, L., 'The 21st Century Maritime Silk Road: Security implications and ways forward for the European Union', SIPRI, Sep. 2018.

an important enabler of military security because the strategy that many European countries are adopting is based on mobilizing and reinforcing small armed forces in a crisis rather than recreating the large standing armies of the cold war era. Given connectivity's relevance to both the military and non-military dimensions of security, the nature and implications of the growing connectivity between the EU and China are under close scrutiny.

While European states do not perceive China as a direct threat, the more prominent role that Chinese companies play in digital and transport networks makes it inevitable that European states are beginning to include China more directly in their thinking as they elaborate their security strategies. That does not mean that China will be a target for security measures or that the relationship will become adversarial. The instruments that are now being designed in European states are careful to avoid being China-specific, but the recalibration of relations with China by the EU and by the North Atlantic Treaty Organization (NATO, to which 21 EU member states are also member) is likely to have an impact on how security measures are implemented at the national level.

Identifying the challenges and risks associated with connectivity will contribute to enabling sustainable EU–China cooperation

A stable EU–China partnership can develop only if security concerns are recognized and addressed. Identifying the challenges and risks associated with connectivity will contribute to enabling sustainable EU–China cooperation. The objective of this paper is to examine the implications of connectivity on evolving EU–China relations, from the European perspective. Section II assesses current EU–China relations and the influence of connectivity; section III outlines the major challenges and risks that Europe is facing in the domain of transport and digital connectivity; section IV explores how infrastructure might affect military security in Europe; section V illustrates the instruments the EU is developing to enhance its security in an era of connectivity; and section VI offers brief conclusions.

II. The changing dynamics of EU–China relations

China and the EU established diplomatic relations in 1975.[3] Their bilateral relations were further developed through trade and evolved into a comprehensive strategic partnership in 2003. This commitment was reinforced in 2013 with the implementation of the 'EU–China 2020 Strategic Agenda for Cooperation'.[4] Under the strategic agenda, China and the EU agreed that they have the responsibility to meet regional and global challenges together as important actors in a multipolar world. To that end, the two sides agreed to enhance their dialogue and ensure that consultations are full and effective on major issues of mutual concern.[5] These consultations include three key dialogue pillars: the annual High-level Strategic Dialogue, the annual High-level Economic and Trade Dialogue and the biannual People-to-People Dialogue.[6]

[3] European Commission, 'EU–China relations', MEMO/95/75, 18 Apr. 1995.
[4] European External Action Service (EEAS), 'EU–China 2020 Strategic Agenda for Cooperation', 23 Nov. 2013.
[5] Hu, W., 'China as a WTO developing member: Is it a problem?', CEPS Policy Insights, no 2019/16, Nov. 2019, p. 17.
[6] Hu (note 5).

Until very recently, the main drivers of EU–China relations have been finance and commerce; for example, the balance of issues in the strategic agenda from 2013 remained firmly weighted towards economic cooperation. However, with the increasing economic and political influence of China as a global actor, the EU has noted 'a growing appreciation in Europe that the balance of challenges and opportunities presented by China has shifted'.[7] The EU has called for change, with greater reciprocity in commerce, improved intellectual property rights protection, increased cooperation on high-end technology and dialogue on economic reform.[8]

Illustratively, French President Emmanuel Macron's statement in March 2019 that 'the relationship between the EU and China must not be first and foremost a trading one, but a geopolitical and strategic relationship' reflects an emerging desire for the EU and its member states to review their current approaches towards China on both political and security fronts.[9]

Notably, recent EU documents on security partnerships touch only briefly on China and tend not to view it as a partner but as a possible security risk. For example, the March 2019 EU strategic outlook document refers to China as a potential security problem.[10] The document points to some Chinese policies that raise security concerns, including 'cross-sectoral hybrid threats' that must be addressed.[11] The EU Global Strategy and 2019 political guidelines are largely silent on China: in the 2016 'Global Strategy for the EU's Foreign and Security Policy' (EU Global Strategy), security relationships in Asia reference partnerships with Japan and South Korea but not China.[12] In the 2019 political guidelines for the new European Commission, priorities are close security partnerships with the USA and the United Kingdom after it leaves the EU.[13]

The issue of connectivity is at the heart of the relationship between the EU and China. In September 2015 China and the European Commission signed a memoranda of understanding (MOU) on establishing a Connectivity Platform to create modern transport infrastructure.[14] The only reference to China in the 2016 EU Global Strategy is to finding 'a coherent approach to China's connectivity drives westwards by maximising the potential of the EU–China Connectivity Platform'.[15]

[7] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (note 1).

[8] On the basis of 'open markets, common standards and joint research on the basis of reciprocity'. European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Elements for a new EU strategy on China', Joint communication to the European Parliament and the Council, JOIN(2016) 30 final, 22 June 2016, p. 9.

[9] Reuters, 'EU leaders call for end to "naivety" in relations with China', 22 Mar. 2019.

[10] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (note 1).

[11] The EU strategic outlook on China was finalized shortly after public reports that hackers orchestrated by Chinese authorities had accessed EU internal communications for 3 years without detection. Sanger, D. E. and Erlanger, S., 'Hacked European cables reveal a world of anxiety about Trump, Russia and Iran', *New York Times*, 18 Dec. 2018; and Jones, C., 'EU communications hack linked to Chinese spies', ITPro, 19 Dec. 2018.

[12] European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger Europe* (EEAS: Brussels, June 2016).

[13] von der Leyen, U., 'A Union that strives for more: My agenda for Europe', 2019.

[14] European Commission, 'The EU–China Connectivity Platform'.

[15] European External Action Service (note 12).

However, as part of broader strategic concerns, the EU has also increasingly viewed Chinese connectivity projects as part of a 'grand strategy' linked to China's industrial and economic policy 'Made in China 2025'.[16] Through this policy, China aims to achieve world-leading standards in high technology across a range of sectors that the EU regards as central to its own future economic, political and strategic well-being.[17] Meanwhile, in China's new 'Policy Paper on the European Union', it has explicitly mentioned that the EU should 'avoid politicizing economic and trade issues, and ensure the sustained, steady and win–win progress of China–EU economic and trade relations'.[18] This has become one of the major elements of divergence between China and the EU, for understanding the development in their bilateral relations.

US influence on EU–China relations

The relationship between China and the EU is in a formative period and has followed a different trajectory from the relationship that China has developed with the USA. It was in the 1990s that the USA began to look beyond commercial relations with China and to assess the wider implications of the rise of a major power with 'sharply contrasting worldviews, competing geo-strategic interests, and opposing political systems'.[19] Over time, a broad consensus has formed across the US Government that China has effectively combined commercial and national security espionage in ways that harm the US economy and defence effort.[20] The USA now believes that regulatory measures specifically targeting China are justified to protect government information and communication systems. The US Government is using incentives and regulations to encourage private sector caution in forming partnerships with Chinese entities.[21]

The EU has not reached the same conclusions as the USA. Although the EU has noted China as an economic competitor in technology and a systemic rival in governance, the wider paradigm for EU–China relations remains finding areas for mutually beneficial cooperation instead of promoting containment.[22] The relationship is not currently adversarial but, partly through its own internal procedures and partly because of the USA's influence, the EU has begun to address the security implications of connectivity in a

[16] Ekman, A. (ed.), 'China's Belt & Road and the world: Competing forms of globalization', IFRI, Apr. 2019; 'Europe has to buckle up to survive the challenge of the "Belt and Road"', MERICS, 30 Sep. 2019.

[17] The sectors identified in Made in China 2025 include: advanced information technology industry, machinery and robotics, aerospace and aeronautic equipment, marine engineering equipment and vessels, advanced rail transport equipment, energy saving vehicles and renewable energy, agricultural machinery and equipment, new materials, biopharma and high-performance medical products. Chinese State Council, [Made in China 2025], 8 May 2015 (in Chinese).

[18] Xinhua, 'Full text of China's policy paper on the European Union', 18 Dec. 2018.

[19] US–China Security Review Commission, *The National Security Implications of the Economic Relationship between the United States and China*, First Annual Report to Congress (US–China Security Review Commission: Washington, DC, July 2002), p. 1.

[20] US–China Economic and Security Review Commission, *2016 Annual Report to Congress* (US–China Economic and Security Review Commission/US Government Publishing Office: Washington, DC, Nov. 2016).

[21] 'BUILD Act: Frequently asked questions about the new US International Development Finance Corporation', Congressional Research Service, 15 Jan. 2019.

[22] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (note 1).

more systematic and serious manner. European analysts such as Corrado Clini, the former Italian minister of environment, have asserted that whether or not Chinese policies are strategic or opportunistic, there is a strong case for greater EU coherence to avoid becoming a 'playground of competition' between China and the USA.[23] However, individual member states have their own interests and operate within their specific context. Several EU member states have signed a MOU with China regarding connectivity; one EU concern is that agreements between China and individual member states, or groups of states, will undermine collective bargaining power and weaken protection against Chinese reprisals if decisions are unpopular in China.[24]

The USA is a crucial security partner for most European states and, therefore, will always be listened to carefully. Some European analysts detect an evolving European view that the new challenge of China should be part of a common transatlantic agenda, and pinpoint a change in perspective by France and Germany as a critical tipping point.[25] The potential for friction on trade issues between the EU and the USA could complicate finding a common approach towards China. However, the current debates are taking place in an increasingly unpredictable geopolitical and strategic environment, where key actors are manoeuvring actively as well as reactively.

The current debates are taking place in an increasingly unpredictable geopolitical and strategic environment, where key actors are manoeuvring actively as well as reactively

The changing nature of connectivity's security dimension

Until recently, the security dimension of EU–China connectivity was focused on the shared interest of protecting transport links and supply chains from terrorism and organized crime. For example, China and EU member states have worked to reduce the threat of piracy at sea within a broad international coalition.[26] While this dimension remains important, the security discourse in Europe has changed significantly since Russia's annexation of Crimea in 2014, and those changes are beginning to have an impact on relations with China in the field of connectivity.

Members of the EU and NATO realized that they were poorly prepared to respond to contingencies of the kind experienced by Ukraine. A new assessment of military risks led to a significant increase in resources allocated to the military, extensive planning to address a range of potential contingencies and an unprecedented level of EU–NATO cooperation. They have begun to design a contemporary form of national and European defence that not only enhances traditional military capabilities but also extends into protecting critical societal functions and infrastructure against the risk of attack

[23] Clini, C., 'The quest for coherence in Europe's connectivity strategy', European Interest, 12 Apr. 2019.

[24] Countries that have currently signed MOUs on the BRI include: Bulgaria [signed in 2015], Croatia [2017], Czech Republic [2015], Greece [2018], Hungary [2015], Italy [2019], Latvia [2016], Poland [2015], Romania [2015] and Slovakia [2015].

[25] Ringsmose, J. and Rynning, S., 'China brought NATO closer together', 5 Feb. 2020.

[26] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (note 1), p. 3.

using non-military instruments such as cybertools, sabotage or chemical, biological or radioactive threat agents.[27]

The EU is now analysing risks and developing common instruments to protect networks across the spectrum of critical infrastructure, transport, energy and telecommunications. Such discussion involves the most important security partners of the EU—first and foremost the USA and European states that are members of NATO but not the EU (including the UK after Brexit), as well as Japan and South Korea, which are viewed as important security partners in Asia.[28] The result of the discussion will inevitably have an impact on future cooperation between China and the EU in the sphere of connectivity and in their broader bilateral relations.

III. The challenges and risks associated with EU–China connectivity

The EU and China are exploring a number of connectivity opportunities, including separately through the BRI and the EU's Connecting Europe Programme, as well together through the EU–China Connectivity Platform. Despite stated aims to synergize these connectivity initiatives, there are also a host of challenges and concerns. The following sections spell out a number of these challenges to greater cooperation between the EU–China as they relate specifically to transport and digital connectivity: first, in the EU's broader political–economic relationship with China, and then with special emphasis on EU concerns as they relate to military mobility.

Overview of some of the key initiatives related to EU–China connectivity

The BRI, which was first announced in 2013, has emerged as the Chinese Government's flagship foreign economic and policy initiative. An umbrella initiative, the BRI has come to encompass a range of Chinese activities that seek to enhance physical, digital and commercial networks across the rest of the world. It has been used to refer to bilateral, multilateral and private sector exchanges between Chinese actors and foreign counterparts. In the absence of a formal definition or list of projects, the BRI has also been used as a shorthand to describe overall Chinese foreign direct investment (FDI) in, and trade with, so-called BRI countries.[29] China has added a digital and information component to the BRI through the Digital Silk Road

[27] In July 2016, the leaders of the EU and NATO signed a Joint Declaration in Warsaw listing 7 areas where cooperation between the 2 organizations should be enhanced: countering hybrid threats; operational cooperation including at sea and on migration; cybersecurity and defence; defence capability development; defence industry and research; exercises; supporting Eastern and Southern partners' capacity building efforts. European Council, 'EU–NATO joint declaration: Joint declaration by the president of the European Council, Donald Tusk, the president of the European Commission, Jean-Claude Juncker, and the secretary general of NATO, Jens Stoltenberg', Warsaw, 8 July 2016.

[28] The 2016 Global strategy for the EU's foreign and security policy makes explicit reference to strengthening security partnerships with Japan and South Korea. European External Action Service (note 12).

[29] This includes by Chinese government bodies: Chinese Ministry of Finance, [Jan.–Oct. 2019 China-BRI countries' investment situation], 21 Nov. 2019 (in Chinese); and Chinese State Information Center, [BRI Trade Cooperation Big Data Report 2018], 8 May 2018 (in Chinese). See also

(DSR), which encompasses cooperation in internet and telecommunication infrastructure, e-commerce and other emerging technology industries.[30]

The EU Connecting Europe programme is a long-term initiative to promote digital, energy and transport networks inside the EU. Within Connecting Europe, the Trans-European Transport Network (TEN-T) will coordinate the development of an EU-wide network of roads, railway lines, canals and coastal shipping routes along with the associated ports, airports and railway terminals. By 2030 the TEN-T plans to deliver a core network focused on the most important elements, and by 2050 a comprehensive network covering all European regions should be in place.[31] The EU has noted the links and potential interoperability between Connecting Europe networks and Asia.[32] In 2015 the EU launched its Digital Single Market strategy to create a single market 'where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection'.[33] The digital dimension of the EU Connecting Europe programme supports and finances the development of building blocks for a digital single market, such as trusted electronic forms of identification, signature, invoicing, blockchain data storage and translation services.[34]

Synergies between the separate connectivity initiatives of China and the EU are being explored via the EU–China Connectivity Platform

Synergies between the separate connectivity initiatives of China and the EU are being explored via the EU–China Connectivity Platform, established in 2015.[35] China and the EU have each nominated pilot transport projects that are open to joint financing and operate on a principle of reciprocity.[36] China has identified Europe as the end destination of both its land-based and maritime BRI routes. In addition, while current Chinese transport projects in the EU do not always map onto planned TEN-T networks, Chinese actors are nevertheless beginning to discuss these projects as complementary to EU initiatives.[37]

Cooperation on digital connectivity is less developed in their discussions than that on transport, but there are a number of dialogue mechanisms and

Hillman, J. E., 'How big is China's Belt and Road?', Center for Strategic and International Studies, Commentary, 3 Apr. 2018.

[30] Yong, H., 'Construction of Digital Silk Road lights up BRI cooperation', *People's Daily*, 24 Apr. 2019.

[31] Regulation (EU) 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 661/2010/EU, *Official Journal of the European Union*, L348, 20 Dec. 2013.

[32] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Connecting Europe and Asia: Building blocks for an EU strategy', Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank, JOIN(2018) 31 final, 19 Sep. 2018.

[33] European Commission, 'A Digital Single Market Strategy for Europe', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2015) 192 final, 6 May 2015.

[34] An online catalogue of digital building blocks is regularly updated at the Connecting Europe Facility website.

[35] European Commission, EU–China Connectivity Platform website.

[36] On the same reciprocity principle, a joint study on sustainable rail-based corridors between Europe and China has been commissioned. See e.g. European Commission, EU–China Connectivity Platform, 'Terms of reference of the joint study on sustainable railway-based comprehensive transport corridors between Europe and China', Annex to the minutes of the 4th Chairs' Meeting, Brussels, 8 Apr. 2019.

[37] Economic analyst, Interview with the authors, Athens, 11 Dec. 2019.

cooperation initiatives, including an ad hoc expert group on cybersecurity and the digital economy.[38] The deployment of fifth generation (5G) network technology has also been recognized as a priority for the digital single market. In 2015 the EU and China signed a joint declaration to promote common global standards, reciprocity and openness in terms of research funding and market access regarding 5G digital networks.[39]

Connecting transport networks

Chinese involvement in the construction of European infrastructure predates the establishment of the BRI, but has accelerated with new land and maritime-based initiatives explicitly aimed at bridging China to Europe.[40] Along maritime routes, China has begun to acquire a stake in ports encompassing at least 10 per cent of Europe's shipping container capacity.[41] While investments such as in Piraeus port in Greece are successful in commercial terms, concerns have been raised by European and US policymakers that these investments could have strategic implications in terms of access and logistical support for military operations. In 2017 the president of the European Commission, Jean-Claude Juncker, expressed that, among other investments, port purchases by foreign, state-owned enterprises (SOEs) should be subject to greater 'scrutiny and debate.'[42]

China's accelerated drive for new foreign markets is driven in part by domestic overcapacity in heavy industry and infrastructure sectors. To some extent, this overcapacity also matches demands in Central, Eastern, South Eastern and Southern Europe. For example, as part of the Connecting Europe programme there is a specific sub-element focused on 12 member states that form a corridor connecting the Baltic Sea, Black Sea and Adriatic Sea (Three Seas initiative). Rail and road travel through this corridor takes on average between two and four times as long as comparable distances in the western and northern parts of Europe. The Three Seas Initiative provides financial support to transport projects intended to reduce the cost and time of moving freight through the north–south corridor inside the EU.[43] Transport agreements have been signed under the framework of the so-called 16+1 mechanism, encompassing 16 Central and Eastern European (CEE) states and China (with the addition of Greece in April 2019 making

[38] European External Action Service, 'The EU and China have launched a series of discussions on economic consequences of cybersecurity policies and success factors for the successful development of the digital economy', 1 Sep. 2016.

[39] European Commission, 'The EU and China signed a key partnership on 5G, our tomorrow's communication networks', Press release, 28 Sep. 2015.

[40] Limited Chinese investments in the sector first began to take place under the framework of China's Going Out strategy (starting in the 2000s), but substantially increased in the aftermath of the global financial crisis. Hanemann, T. and Huotari, M., *EU–China FDI: Working Towards Reciprocity in Investment Relations*, MERICS Papers on China no. 3 (Mercator Institute for China Studies: Berlin, May 2018).

[41] Merk, O., 'Geopolitics and commercial seaports', Revue Internationale et Strategique No. 107 (2017); and Huang, K., 'Why China buying up ports is worrying Europe', South China Morning Post, 23 Sep. 2018.

[42] European Commission, 'State of the Union 2017', Press release, 14 Sep. 2017; and US Department of Defense, 'Assessment on US defense implications of China's expanding global access,' Dec. 2018, p. 4.

[43] European Commission, 'The Three Seas Initiative summit: European Commission investments in connectivity projects', Bucharest, 17–18 Sep. 2018.

it 17+1). Discussing connectivity in a framework that includes EU member states and non-member states introduces some additional complications if projects are to be linked to EU planning and financing instruments.

There is, for example, both Chinese and EU interest to improve connections between Greece and Central Europe. Potential pilot projects within the framework of the EU–China Connectivity Platform could form the basis for a more integrated approach. However, among the difficulties in that regard are that China and the EU do not fully coordinate plans, including routes. It is also unclear how grants under EU financial instruments such as the Instrument for Pre-Accession will be combined with loans from EU institutions, Chinese banks and international financial institutions. There is a need to address contradictions among transport projects in South Eastern Europe by assessing them by type, sequence and financing by both China and the local authorities.

Integrated planning and governance concerns

The decision to build a Belgrade–Budapest rail link, for example, has been criticized on the basis that it primarily serves Chinese interests in moving goods quickly to markets in central Europe. The route of the new railway will not serve some important Hungarian towns and cities and no plan to connect the railway to the port of Piraeus has been agreed.[44]

Some countries that are important to the TEN-T core network development aspire to become EU member states. In the Western Balkans, for example, cooperation with China on connectivity has become entangled with discussions about future EU membership.[45] States that seek EU membership must progressively align their regulations and practices with EU rules, but China applies different standards. If the availability of Chinese funding that can be more quickly disbursed dilutes the application of EU-based rules, the accession process may be delayed. Moreover, if states in the Western Balkans perceive that the EU is backing away from commitments to promote their candidacies for EU membership, they may look to cooperate more closely with China.

Chinese investments are often conducted through SOEs, which have a mixture of commercial and policy drivers and have access to state financing and subsidies. Loans provided to European projects by Chinese policy banks are often conditional on the majority of funds being returned to Chinese construction companies.[46] Thus, calls for a more level playing field feature strongly in EU responses to Chinese connectivity projects.[47] The European Commission has argued for connectivity projects to be seen in the wider context of reciprocity.[48]

[44] Prager, A., 'Budapest–Belgrade railway: Orbán flirts with China', Euractiv, 23 Sep. 2019.

[45] While there is no official definition of the Western Balkans, for the purposes of this paper it refers to Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia. Holzner, M. and Schwarzhappel, M., *Infrastructure Investment in the Western Balkans: A First Analysis* (European Investment Bank and the Vienna Institute for International Economic Studies: Luxembourg/Vienna, Sep. 2018).

[46] Ghossein, T., Hoekman, B. and Shingal, A., *Public Procurement in the Belt and Road Initiative*, MTI Discussion Paper no. 10 (World Bank: Washington, DC, Dec. 2018).

[47] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (note 32).

[48] Juncker, J.-C., Remarks of President Juncker at the joint press conference with Mr Li Keqiang, Premier of the State Council of the People's Republic of China, and Mr Donald Tusk, President of the

Existing projects have also raised concerns related to economic and corporate governance, both of recipient EU member states and of Chinese actors. Hungary awarded the contract to build the railway to the China Railway International Corporation, financed by a loan from the Export–Import Bank of China, without a public tender. The European Commission is investigating whether the process infringed EU rules.[49]

Chinese investment and funding practices have also raised questions regarding recipient country debt. In Montenegro, the Bar–Boljare Highway Project, financed by the China Export–Import Bank, has played a role in the sharp increase in the country's public debt since 2017.[50] With a few high-profile exceptions, asset seizures have not featured prominently in Chinese loans abroad.[51] And while debt non-repayment negatively impacts the investor as well as the recipient, European narratives perhaps understandably exhibit concern over the possibility of predatory lending. In response to international debt-related concerns, the Chinese Ministry of Finance has recently released a non-mandatory BRI 'Debt Sustainability Framework' to help to guide and ensure more sustainable investment and lending decisions.[52]

Existing projects have also raised concerns related to economic and corporate governance, both of recipient EU member states and of Chinese actors

Finally, while all investment projects are expected to comply with recipient country legislation, it is worth noting that EU environmental impact standards (EIAs) are variably applied within member states.[53] Thus, the fact that the environmental policies of Chinese policy banks remain less stringent than those of other international and multilateral financial institutions can potentially have implications for environmental and social sustainability.[54] EU and Chinese partners have made commitments to develop and promote green smart transport infrastructure via the EU–China Connectivity Platform, but this commitment will continue to come under scrutiny as data on China's overseas investments and lending activities shows that they remain significantly oriented towards carbon-intensive rather than green projects.[55]

European Council, Brussels 9 Apr. 2019.

[49] Beesley, A., Byrne, A. and Kynge, J., 'EU sets collision course with China over "Silk Road" rail project', *Financial Times*, 20 Feb. 2017.

[50] The International Monetary Fund (IMF) estimates that the first phase of the project has raised government debt to a projected 82% of gross domestic product, versus 59% without it. IMF, *Montenegro: Staff Report for the 2019 Article IV Consultation*, IMF Country Report no. 19/23 (IMF: Washington, DC, Aug 2019); Shepard, W., 'Another Silk Road fiasco? China's Belgrade to Budapest high-speed rail line is probed by Brussels' Forbes, 25 Feb. 2017; and Barkin, N. and Vasovic, A., 'Chinese "highway to nowhere" haunts Montenegro', Reuters, 17 July 2018.

[51] Kratz, A., Feng, A. and Wright, L., 'New data on the "debt trap" question', Rhodium Group, 29 Apr. 2019.

[52] Chinese Ministry of Finance, 'Debt sustainability framework for participating countries of the Belt and Road Initiative', 25 Apr. 2019.

[53] European Commission, 'Impact assessment summary: Executive summary of the impact assessment accompanying the document proposal for a directive of the European Parliament and of the Council amending Directive 2011/92/EU on the assessment of the effects of certain public and private projects on the environment', SWD(2012)354/F1, 26 Oct. 2012.

[54] Losos, E. et al., *Reducing Environmental Risks from Belt and Road Initiative Investments in Transportation Infrastructure*, Policy Research Working Paper no. 8718 (World Bank: Washington, DC, Jan. 2019).

[55] European Commission, EU–China Connectivity Platform, 'Meeting minutes of the 4th Chairs' Meeting of the EU–China Connectivity Platform', Brussels, 8 Apr. 2019; Kong, B., and Gallagher, K. P., *Globalization as Domestic Adjustment: Chinese development Finance and the Globalization*

China has begun to address many of the criticisms of BRI projects, as many of the identified risks and challenges outlined herein negatively affect the broader sustainability of Chinese investments as well. This includes the adoption of more stringent regulatory guidance, standards and principles for BRI-related projects.[56] China and the EU are increasingly exploring mixed sources of funding and deeper coordination among financing institutions, which should further promote compatibility in the transport sector.[57]

Digital connectivity

The EU identifies digital technology as transformative. In its Digital Single Market strategy, the European Commission states that 'Information and Communications Technology (ICT) is no longer a specific sector but the foundation of all modern innovative economic systems'.[58] As previously noted, the Connecting Europe programme is expected to help ensure that the EU remains at the forefront in the development and exploitation of digital technology.

The future 5G network that will be a key element of the Digital Single Market will evolve from the existing 3G and 4G networks in Europe that China has been a partner in building. Until recently, China's involvement in building 5G networks in Europe had been assumed, but during 2019 political attention started to focus on challenges and potential risks in the digital sector.

Risks and challenges of digital connectivity

In October 2019 the EU released a coordinated risk assessment report for 5G networks, based on contributions from the national risk assessments of member states. Four categories of risk were identified: (*a*) the disruption of local or global 5G networks; (*b*) spying on traffic carried by a network; (*c*) the modification of the data in a network; and (*d*) the destruction or alteration of physical infrastructure caused by action through the network.[59]

These threats could compromise the availability, confidentiality or integrity of data in ways that deny essential network services. However, the risk assessment report notes that threats could emanate from diverse sources, including individual hackers, terrorist groups, organized crime groups, insiders, state actors (or state-backed non-state actors) and corporate entities. The security concerns are not linked to China specifically, but many of the points contained in EU guidelines on constructing risk profiles are likely to focus attention on transactions involving Chinese entities. These risk profiles could include an assessment of the following: (*a*) the potential

of China's Coal Industry, Boston University Global Development Policy Center, Working Paper no. 6, Apr. 2019; and Zhou, L. et al., *Moving the Green Belt and Road Initiative: From Words to Action*, Working Paper (World Resources Institute: Washington, DC, Oct. 2018).

[56] Chinese Ministry of Finance (note 52); and People's Republic of China, Ministry of Ecology and Environment, 'Guidance on promoting green Belt and Road', 28 June 2017; and Hou L., 'China officially launches green development coalition under BRI', China Daily, 25 April 2019.

[57] Interview with the authors (note 37); and Asian Infrastructure Investment Bank (AIIB), 'Memorandum of understanding on collaboration on matters to establish the Multilateral Cooperation Center for Development Finance', 25 Mar. 2019.

[58] European Commission (note 33), p. 3.

[59] NIS Cooperation Group, *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks* (European Union Agency for Cybersecurity: Heraklion, 9 Oct. 2019).

exploitation of weaknesses or vulnerabilities by a dominant supplier and the potential risks along supply chains if an important supplier is involved in many critical information technology (IT) applications; (*b*) the risk of interference where there is a strong link between the supplier and a government of a given third country (i.e. non-EU member state); (*c*) the extent to which the legislation in the given third country lacks legislative or democratic checks and balances; (*d*) whether the EU and the given third country have security or data protection agreements; (*e*) whether the corporate ownership of the supplier gives a third-country government a role in decision making; and (*f*) whether the given third country can create pressure in relation to the place of manufacturing of key equipment. [60]

In addition, since 2018, European rules on data protection emphasize the individual right to privacy, and require any holder of personal information to obtain consent from the owner before using their data. The right to privacy applies wherever in the world information about an individual is held. European Parliament concerns stem from the fact that Chinese and EU approaches to data protection are not harmonized.

European Parliament's concern over political influence

The European Parliament has become an increasingly important actor in the creation and implementation of EU policies, particularly if legislative action or the use of the EU common budget is envisaged. Notably, in a 2018 resolution on the state of EU–China relations, the European Parliament highlighted what it described as the 'largely ignored' process by which the Chinese leadership has 'gradually and systematically stepped up its efforts to translate its economic weight into political influence' in Europe.[61]

In 2019 the European Parliament made its security concerns related to the future 5G network more explicit and drew attention to allegations that 5G equipment developed by Chinese companies 'may have embedded back-doors that would allow manufacturers and authorities to have unauthorised access to private and personal data and telecommunications from the EU'.[62] The European Parliament expressed concerns that China would extend the 'sophisticated network of invasive digital surveillance' practised at home to monitoring Chinese citizens or other individuals of interest while inside the EU.[63]

IV. The influence of military factors on EU connectivity

After 2014 the military factor became much more important in European thinking about security, and EU and NATO member states developed new plans that emphasize national and collective defence against a sophisticated state adversary. Those plans are now being implemented and connectivity is an important element in strengthening European military security.

[60] NIS Cooperation Group (note 59).

[61] European Parliament Resolution of 12 September 2018 on the state of EU–China relations (2017/2274(INI)), 12 Sep. 2018.

[62] European Parliament Resolution of 12 March 2019 on 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)), 12 Mar. 2019.

[63] European Parliament Resolution of 18 April 2019 on China, notably the situation of religious and ethnic minorities (2019/2690(RSP)), 18 Apr. 2019.

As noted above, the EU and NATO have recently expanded their cooperation on security issues and consolidated their working procedures at all levels. Each is making an assessment of the impact of China on their security concerns.

In 2017, the US Secretary of Defense, James Mattis, introduced addressing 'a more assertive China' into the NATO discourse. Mattis suggested that a transatlantic approach to China would be in the shared interest of NATO members.[64] In April 2019 NATO began to prepare the confidential paper 'Understanding China Better', which was considered by NATO leaders at the end of the year.[65] In December 2019 NATO leaders agreed to initiate a forward-looking reflection exercise of which the implications of growing Chinese influence would be one part.[66] According to NATO Secretary General Jens Stoltenberg, 'this is not about moving NATO into the South China Sea, but it's about taking into account that China is coming closer to us—in the Arctic, in Africa, investing heavily in our infrastructure in Europe, in cyberspace'.[67]

New military policies and plans

EU and NATO member states have developed new plans that emphasize national and collective defence against a sophisticated state adversary, and connectivity is an important element

In 2014 the EU, and indeed most states in Europe, suffered a strategic shock when Russia used military means to annex part of the territory of neighbouring Ukraine. European states realized that if they were directly affected by a similar event, they would be completely unprepared. After reducing their investments in the military and reconfiguring their armed forces for stabilization and peace operations (most of which were outside Europe) during the 1990s, EU and NATO member states had little capability for territorial defence. Russia, on the other hand, appeared much better prepared having invested in a significant military reform and modernization programme after 2008.

EU and NATO member states do not plan to recreate the static force posture of the cold war, during which massive military formations were permanently stationed close to borders that were considered particularly vulnerable to invasion. Rather than the Europe-wide scenario that was the basis for cold war planning, the revived force posture is first and foremost designed to address conflict scenarios at the local or regional levels.[68] Responses should be adjustable to the scale of the challenge across a spectrum of contingencies, from local and low-intensity conflict to high-intensity warfare. The concept places a heavy emphasis on fast troop deployments and a reliable, capable transport infrastructure that will function in conditions of crisis and conflict.[69] Furthermore, the scenarios anticipate various forms of disruption,

[64] US Mission to the North Atlantic Treaty Organization, 'Intervention by US Secretary of Defense Jim Mattis: Session one of the North Atlantic Council', 15 Feb. 2017.

[65] Ringsmose, J., and Rynning, S., 'Kina tvinger NATO til at tænke nyt' [China is forcing NATO to rethink], *Berlingske*, 2 Dec. 2019.

[66] Kempe, F., 'NATO's China challenge', Atlantic Council, 7 Dec. 2019.

[67] Rosenthal, M. J., 'NATO secretary general: The Alliance is delivering', Atlantic Council, 3 Dec. 2019.

[68] NATO, *NATO: Ready for the Future: Adapting the Alliance (2018–2019)* (NATO: Brussels, 2019).

[69] Dalsjö, R. et al., 'Deterrence by reinforcement: The strengths and weaknesses of NATO's evolving defence strategy', Swedish Defence Research Agency Report FOI-R--4843--SE, Nov. 2019.

from cyberattacks on digital networks to the use of chemical threat agents and potential civil disorder.

European planning for military mobility is not exclusively focused on moving forces into Europe; it also takes into account possible future actions elsewhere. Most missions under the EU Common Security and Defence Policy have been to the south of the EU, and the possibility of additional joint efforts has been promoted by leaders, including President Macron.[70] In 2011 NATO carried out Operation Unified Protector in Libya, and whether NATO 'could contribute more to regional stability and the fight against international terrorism' in the Middle East was discussed at the December 2019 London Summit.[71]

The potential for actions to the south, east or south east focuses military mobility planning on key locations in the Baltic states, Poland, Romania and along the Mediterranean coast. Therefore, the fact that Chinese SOEs now have investments of varying size in 12 seaports in the EU has assumed significance in the overall assessment of military mobility planning.[72]

The force mobilization and reinforcement plans on which the emerging strategy depends generate a large body of information that needs to be protected. Since a growing share of information is created and stored in digital form, ensuring the integrity and security of networks is now essential. Moreover, it is not sufficient to apply security measures to dedicated military networks. Modern communication networks that were built for civilian use are an integral part of military mobilization plans. For example, over 90 per cent of deployment and information distribution transactions by the US Transportation Command move through partly or fully unclassified networks and depend on the cybersecurity capabilities of commercial partners.[73] Plans for reinforcement and mobility are a high-value target for potential adversaries because they indicate when and where armed forces will be located at a given time. In 2013 the Commander of the US Transportation Command informed Congress of more than 180 000 cyberattacks during 2012.[74]

Military plans are beginning to have an impact on thinking about digital connectivity. Protecting mission data on digital networks is an extremely high priority and, as noted above, this protection must extend to civilian networks owned and operated by commercial entities to ensure information security. Where Chinese companies are key suppliers of equipment to civilian digital networks, they naturally become subject to cybersecurity and information security assessment.

[70] In September 2017 President Macron proposed that his European Intervention Initiative, in which states coordinate their voluntary contributions to military actions, should evolve into a common EU intervention force. Macron, E., 'Initiative for Europe', Speech, Sorbonne, Paris, 26 Sep. 2017.

[71] Herszenhorn, D. M., 'Trump asks for NATO help in the Middle East', *Politico*, 8 Jan. 2020.

[72] The 12 ports are located in Belgium, France, Greece, Italy, the Netherlands and Spain. In addition to investments inside the EU, China has also invested in the Turkish Kumport on the coast of the Sea of Marmora close to Istanbul. Kakissis, J., 'Chinese firms now hold stakes in over a dozen European ports', *NPR*, 9 Oct. 2018; and 'Turkey sees a sudden spike in Chinese investments through "Belt and Road Initiative"', *Daily Sabah*, 30 June 2018.

[73] Fraser, W. M., United States Transportation Command, Statement before the US Senate Armed Services Committee, Washington, DC, 7 Mar. 2013.

[74] Reed, J., 'US Transportation Command hit with 180,000 cyber attacks last year', *Foreign Policy*, 8 Mar. 2013.

Creating the infrastructure, command structures, processes and plans needed to generate combat formations and move them quickly is also very challenging. Current defence planning anticipates being able to deploy multiple brigade- and division-sized formations by 2030 if necessary. The formations will include multinational units combining European national forces, but reinforcements from the USA will also play a major role.[75]

Similar to cybersecurity and information security, troops, equipment and necessary logistics supplies do not move exclusively through dedicated military infrastructure. Civilian ports, airfields, railway systems and road networks also play a central role in moving forces to where they need to be as quickly as possible.[76] The plans for troop movements generate a large body of information that needs to be protected, and where Chinese companies are engaged into transport networks they will also become subject to security assessments.

Military plans are also beginning to have an impact on transport infrastructure that was designed for civilian purposes. The TEN-T plans for transport networks described above were made to reduce traffic congestion and accelerate the movement of commercial goods within the EU single market. However, the TEN-T plans now include an explicit military dimension, discussed further below.

EU–NATO cooperation

The issues of cybersecurity and enhanced military mobility are prominent in the unprecedented levels of cooperation between the EU and NATO since 2014.

The EU and NATO have concluded a Technical Arrangement on Cyber Defence that will promote joint activities and exchanges between the NATO computer incident response capability (NCIRC) and the Computer Emergency Response Team for the EU (CERT-EU).[77] Strengthening national response capabilities of EU and NATO member states in case of a cyber incident as well as promoting education and training to increase the level of cybersecurity across the public and private sectors are high priorities for this joint effort.

Through the Structured Dialogue on Military Mobility launched in November 2018, the EU and NATO have begun to coordinate activities based on technical specifications developed after 2014. A lot of the work to close identified gaps in transport infrastructure to enhance military mobility will be the responsibility of individual EU and NATO member states, but the EU

[75] In 2020 the US Army will carry out the Defender Europe 20 exercise to practise moving a combat ready division from the US mainland to Poland. The US exercise will be coordinated with a series of European exercises to generate the largest force mobilization since the end of the cold war. The forces will enter Europe through six seaports and six airports prior to forward movement by rail and road. US Army Europe, 'Defender-Europe 20'. The exercise will also test the development of NATO's new Joint Support and Enabling Command, which is the part of the command structure responsible for coordinating rear area activities on behalf of the Alliance.

[76] Coordinating both security and enablement is the task of the NATO Joint Support and Enabling Command that was created in Feb. 2018, and that reached operational status in 2019. Boeke, S., 'Creating a secure and functional rear area: NATO's new JSEC Headquarters', *NATO Review*, 13 Jan. 2020.

[77] European External Action Service, 'EU and NATO increase information sharing on cyber incidents', Press release, 10 Feb. 2016.

will support the effort.[78] The Connecting Europe programme now addresses military mobility directly, including through tabletop exercises that focus on the role of TEN-T projects.[79]

The EU will probably make a significant financial commitment to transport infrastructure to promote military mobility. A funding instrument for the Connecting Europe programme, the Connecting Europe Facility (CEF), will provide financing for TEN-T projects after 2021. The budget proposal that the European Commission prepared for the period 2021–27 included €6.5 billion set aside for projects aimed specifically at adapting transport networks to facilitate military mobility.[80] However, this amount was reduced to €2.5 billion during the intergovernmental negotiations on the budget framework and further reductions cannot be excluded.[81] The CEF is a co-funding instrument, and so financial provision of around €5 billion will probably be leveraged as states make matching contributions. Furthermore, the European Commission has proposed the relaxation of funding rules in other financial instruments to allow EU member states to reallocate cohesion funds to transport infrastructure projects that enhance military mobility. In this case, EU financing could cover up to 85 per cent of the cost of a project.[82]

While the military plans that European states are now making were not designed to combat a threat from China, future Chinese investments may be subject to new kinds of security assessments

The impact of military mobility planning on EU–China relations

The implementation of military plans in Europe is beginning to create ripple effects of different kinds. Projects that were conceived with purely civilian objectives in the past now take account of their potential to enhance military mobility. The fact that digital and transport networks have a dual function means that cybersecurity and information security instruments will need to take account of the protocols developed in the military as well as the civilian sectors.

The military plans that European states are now making were not designed to combat a threat from China. However, future Chinese investments may be subject to new kinds of security assessments, discussed further in the next section.

V. Instruments to enhance EU security in an era of connectivity

The EU has begun to develop a range of instruments that are intended to reduce and manage security risks that might arise from greater connectivity. These instruments are being discussed in a framework that includes

[78] Council of the EU, 'Annexes to the "Military requirements for military mobility within and beyond the EU"', 13674/18, 9 Nov. 2018.

[79] NATO, 'Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 Dec. 2016 and 5 Dec. 2017', 17 June 2019.

[80] European Commission, 'EU budget for the future: Connecting Europe Facility', 2 May 2018.

[81] Brzozowski, A., 'Faced with defence budget threats, EU eyes new money sources', *Euractiv*, 11 Dec. 2019.

[82] Brazys, A., 'Dual-use infrastructure funding through the Connecting Europe Facility', Presentation to the International Union of Railways (UIC) Railway Asset Management Global Conference 2019, Paris, 17–19 Apr. 2019.

transatlantic partners, key partners in Asia and important private sector actors. However, China has not been invited to participate in any of the discussions. The consultations may produce agreed principles, regulations, standards and certification procedures. Although China will not have participated in the development of these measures, they will apply to Chinese companies participating in European infrastructure projects.

Prague 5G Security Conference

On 3 May 2019 representatives from 32 countries met in Prague to discuss guidelines on how to decrease the security risks associated with developing, deploying, operating and maintaining complex communication infrastructures such as 5G networks.[83] The EU, NATO and representatives of four telecommunication network operators also participated in the meeting. The participants from Asia were Australia, Japan and South Korea.

The meeting was convened by the Czech Government to discuss a coordinated approach to protecting telecommunication infrastructure from cyber threats, and the Czech prime minister, Andrej Babiš, explained that the objective was to promote the shared interests of EU member states and NATO members as well as their global partners.[84] At the end of the conference the participants agreed a set of principles, non-binding policy recommendations and guidance on good practice related to the cybersecurity of communication networks in a globally digitalized world.[85] The Czech Government also committed to facilitating follow-up steps.

Strengthening cybersecurity in the EU

In 2016, EU member states agreed that more needed to be done to ensure equal levels of protection to consumers and businesses against cyber risks, and that existing capabilities could not ensure a high enough level of security of network and information systems across the EU. To that end, the so-called Network and Information Security (NIS) Directive included a requirement for every member state establish a national strategy on the security of network and information systems including 'appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems' covering a set of sectors and services agreed at EU level.[86]

The NIS Directive requires the collection of a large volume of information in each member state, and the designation of a single point of contact to receive that information. The national contact points participate in the NIS

[83] Czech Government, 'Prague 5G Security Conference announced series of recommendations: The Prague Proposals', Press release, 3 May 2019.

[84] Czech Government, 'PM Babiš: By protecting the 5G network, we will be protecting the very fabric of our societies, our ability to thrive, even to exist', Opening remarks by Prime Minister Andrej Babiš at the Prague 5G Security Conference, 2 May 2019.

[85] Czech Government, 'The Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitalized world', Prague 5G Security Conference, 3 May 2019.

[86] 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, *Official Journal of the European Union*, L194/1, 19 July 2016.

Cooperation Group, along with representatives of the European Commission and the EU Agency for Cybersecurity (ENISA). The NIS Cooperation Group is a place where member states can share and analyse national information, identify good practice and better understand the impact of cyber incidents with a significant impact. Member states are also obliged by the Directive to create computer security incident response teams (CSIRTs).

Certification of equipment

In 2019 the EU Cybersecurity Act was agreed to address security challenges posed by the increasing number and diversity of devices connected digitally as the faster data transfer speeds 5G networks provided become available.[87] The act envisages a comprehensive certification scheme to raise confidence that a networked product, service or process can be trusted.

At present, EU member states decide whether to implement national certification. Under the Cybersecurity Act it will be mandatory for all member states to introduce national technical regulations. They will also be required to establish a national cybersecurity certification authority. In parallel, ENISA will oversee and coordinate the development of a cybersecurity certification scheme that EU member states will be able to use.

EU member states and ENISA are developing sectoral certification frameworks to be adopted by the European Commission through implementing acts. Each certification framework will create a comprehensive set of rules, technical requirements, standards and procedures at EU level to evaluate specific products or services. EU security certificates will be recognized in all EU member states, but using them will be voluntary, and a process for mutual recognition of national certificates will also form part of the overall framework.

The Cybersecurity Act also encourages producers to use the certification framework when designing new products. If companies developing products, services or processes implement 'security by design' by taking account of certification requirements, they should both ease their subsequent regulatory burden and reduce the risk that users of their products will fall victim to cyber incidents.

Taken together, the measures under the Cybersecurity Act will specify assurance levels for cybersecurity and a system under which suppliers can state that their products conform to a given level. The certification framework will be agreed by representatives of EU member states along with the European Commission and ENISA, but a Stakeholder Cybersecurity Certification Group will provide information and advice during the process. This group will be composed from representatives of European academic, industry and trade associations alongside the various European standards authorities in relevant technical areas.[88]

[87] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 Apr. 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) 526/2013, *Official Journal of the European Union*, L151, 7 June 2019.

[88] European Commission, Stakeholder Cybersecurity Certification Group: Terms of reference, 23 July 2019.

Chinese authorities and companies will not play any role in developing the certification framework, but companies will have to comply with it if they are to sell products in the EU.

Screening foreign direct investment

In a 2017 communication to EU member states and the European Parliament, the European Commission underlined that the EU will remain open to foreign investment, but encouraged policies that protect EU assets against 'takeovers that could be detrimental to the essential interests of the EU or its Member States'.[89]

In March 2019 the EU enacted a regulation that establishes a framework for screening FDI into the EU against security-related criteria such as 'access to sensitive information, including personal data, or the ability to control such information'.[90] Screening mechanisms will comprise criteria that include ownership and control by a non-EU government within the risk assessment. The national legal base in the state where a potential investor is incorporated is one criterion. The degree to which the Chinese Government is able to exert influence over private companies is certain to be a factor during screening.

In March 2019 the EU enacted a regulation that establishes a framework for screening FDI into the EU against security-related criteria such as 'access to sensitive information, including personal data, or the ability to control such information'

EU member states have the main responsibility for implementing the March 2019 regulation, which does not specify in detail what actions are essential at the national level. EU member states can develop measures tailored to their existing legal and administrative frameworks, but they must all designate an authority responsible for risk screening, and design methodologies for risk assessment. The regulation includes provisions for regular consultation and information exchange with the aim of reducing the likelihood that national implementation will be fragmented in ways that reduce the EU screening system's overall effectiveness.

The screening framework is intended to encourage investment while protecting EU strategic interests, and the EU continues to promote mechanisms to increase FDI—which is expected to play an important role in the economic policy of member states.[91] Several European industrial associations have supported the FDI screening mechanism.[92]

[89] European Commission, 'Welcoming foreign direct investment while protecting essential interests', Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2017) 494 final, 13 Sep. 2017, p. 6.

[90] 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, *Official Journal of the European Union*, L79I, 21 Mar. 2019, Article 4(1)(d).

[91] See e.g. the World Bank's case study of CzechInvest as a successful model to compete for FDI. World Bank, Multilateral Investment Guarantee Agency and Foreign Investment Advisory Service, *Competing for FDI* (World Bank: Washington, DC, 2005), pp. 9–45.

[92] E.g. AEGIS Europe, an umbrella organization of 25 European industrial associations, voiced its support in its comments on the draft screening mechanism. AEGIS Europe, 'Commission's proposal establishing a framework for screening of foreign direct investments into the EU: AEGIS Europe position', Feb. 2018. See also Confindustria, 'Italy, Europe and China: Recommendations for a new cooperation strategy', 2019.

The effectiveness of screening mechanisms will partly depend on the quality of information available about FDI transactions. An Offshore Financial Centre can be an investor, which can make it almost impossible to identify the true beneficial owner of an asset. However, to the extent that financial data that is available can be regarded as indicative, more than 20 per cent of inflows into Offshore Financial Centres that acquired EU assets in 2016 were from China and Hong Kong. To uncover true beneficial ownership in FDI, a more forensic analysis of transactions would need to be an element in screening.[93]

The EU has a single market for investment and does not restrict financial flows between member states. The question of how to screen investments in a member state by a company in another member state when the investor is a subsidiary of a non-EU company remains to be resolved.

The degree to which screening mechanisms will take account of military factors is also still to be determined. The defence ministries of China and Russia are currently negotiating a new bilateral agreement.[94] This, and particularly the approach to sharing information, will be heavily scrutinized in Europe. General Curtis Scaparrotti, the former Commander of US European Command and Supreme Allied Commander Europe within NATO, has noted that China's activities in Europe are now being monitored as it seeks to 'secure access to strategic geographic locations and economic sectors through financial stakes in ports, airlines, hotels, and utility providers' while 'Russia and China have increased their transactional collaboration based on some common objectives and opportunities'.[95]

VI. Conclusions

In their 2020 strategic agenda for cooperation, China and the EU agreed that they have the responsibility to meet regional and global challenges together as important actors in a multipolar world. To that end, the two sides agreed to enhance their dialogue and ensure that consultations are full and effective on major issues of mutual concern. The agenda for strategic cooperation pre-dates the significant increase in European attention to security. The increasing connection between the military and non-military dimensions of security have prompted European states to develop new instruments to address potential threats to transport and digital communications networks.

The EU's approach to managing security risks in relation to connectivity does not include country blacklists or to exclude by name any companies from European projects. Rather, the approach is criteria-based and EU member states will be expected to create national laws and regulations that cover the possibility of excluding any non-EU actor from a connectivity project based on risk-screening. This could include China.

EU member states are at varying stages in their development of these national risk-based screening mechanisms. Some member states have existing systems that will need to be modified, while other states will have

[93] European Commission, 'Foreign direct investment flows: Statistics explained', July 2019.

[94] Kashin, V., 'Russia and China take military partnership to new level', *Moscow Times*, 23 Oct. 2019; Xinhua, 'China, Russia pledge to deepen military cooperation', 5 Sep. 2019.

[95] Scaparrotti, C. M. (Gen.), Commander, United States European Command, Statement before the US Senate Armed Services Committee, Washington, DC, 5 Mar. 2019, pp. 9–10.

to create systems from scratch. Over time, national systems will probably converge around a set of standards agreed at the EU level.

China and the EU have derived mutual benefits from their partnership in the past, and neither seeks confrontation or an adversarial relationship in the future. To promote continued cooperation, China and the EU should not ignore the significant changes in the context of their relationship with regard to connectivity-related projects. Where a problem has been identified in implementing the BRI, for example in relation to public debt or respect for environmental regulations, China has begun to examine a solution acceptable to all parties. The same willingness to seek agreed solutions can be applied to other identified and emerging security problems.

To promote continued cooperation, China and the EU should not ignore the significant changes in the context of their relationship with regard to connectivity-related projects

The enhanced coordination on strategic, political and security issues called for within the EU–China High-level Strategic Dialogue could provide a platform for encouraging honest and open discussion of the impact of changes in the international environment on EU–China cooperation. The High-level Strategic Dialogue, for instance, could provide guidance for a more detailed examination of the issues discussed in this paper, as part of the evolving EU–China relationship in an era of connectivity.

Abbreviations

BRI	Belt and Road Initiative
CEE	Central and Eastern European
CEF	Connecting Europe Facility
CERT-EU	Computer Emergency Response Team for the EU
CSIRTs	Computer security incident response teams
DSR	Digital Silk Road
EEAS	European External Action Service
EIAs	Environmental Impact Standards
ENISA	EU Agency for Cybersecurity
EU	European Union
FDI	Foreign direct investment
ICT	Information and communications technology
IMF	International Monetary Fund
MOU	Memoranda of understanding
NATO	North Atlantic Treaty Organization
NIS	Network and information security
NCIRC	NATO computer incident response capability
SOE	State-owned enterprise
TEN-T	Trans-European Transport Network
5G	Fifth generation

RECENT SIPRI PUBLICATIONS

Estimating the Arms Sales of Chinese Companies
Dr Nan Tian and Fei Su
SIPRI Insights on Peace and Security
January 2020

Framing and Responding to Climate-related Security Risks in Swedish Development Cooperation
Dr Malin Mobjörk and Dr Veronica Brodén Gyberg
SIPRI Insights on Peace and Security
January 2020

Arms Flows to South East Asia
Siemon T. Wezeman
SIPRI Report
December 2019

Challenges to Multilateral Export Controls: The Case for Inter-regime Dialogue and Coordination
Kolja Brockmann
SIPRI Report
December 2019

Detecting, Investigating and Prosecuting Export Control Violations: European Perspectives on Key Challenges and Good Practices
Dr Sibylle Bauer and Mark Bromley
SIPRI Report
December 2019

The SIPRI Top 100 Arms-producing and Military Services Companies, 2018
Dr Aude Fleurant, Alexandra Kuimova, Dr Diego Lopes da Silva, Dr Nan Tian, Pieter D. Wezeman and Siemon T. Wezeman
SIPRI Fact Sheet
December 2019

The Geopolitics of a Changing Arctic
Ekaterina Klimenko
SIPRI Background Paper
December 2019

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

SIPRI INSIGHTS ON PEACE AND SECURITY NO. 2020/3

EU SECURITY PERSPECTIVES IN AN ERA OF CONNECTIVITY: IMPLICATIONS FOR RELATIONS WITH CHINA

IAN ANTHONY, JIAYI ZHOU AND FEI SU

CONTENTS

ABOUT THE AUTHORS

Dr Ian Anthony (United Kingdom) is Director of SIPRI's European Security Programme. He has published numerous books on issues related to arms control, disarmament and export control.

Fei Su (China) is a Researcher with SIPRI's China and Asia Security Programme. Her research interests focus on regional security issues in East Asia with a special interest in North Korea, China's foreign and security policy, and maritime affairs. She is also interested in the field of geo-economics and is currently working on the implications of connectivity to EU–China relations.

Jiayi Zhou (United States) is a Researcher in SIPRI's Climate Change and Risk Programme. Before joining SIPRI, she worked as a policy analyst on US–China nuclear relations. Her current research relates to non-traditional security, and the interaction between geopolitics and sustainable development.