FONDATION ROBERT SCHUMAN

POLICY PAPER

Schuman Paper
n°816
13th January 2026

Earl WANG

European Strategic Formulation on Tech Security vis-à-vis China

[1] Not only the US, but the EU and its Member States are also facing Chinese restrictions on foreign critical tech infrastructure. European telecom companies such as *Nokia* and *Ericsson* witness a drop by two-thirds in their market shares in China as compared to 2020. On the other way around, Chinese 'high-risk suppliers' of telecom networks such as *Huawei* and *ZTE* only encountered a 5-10% decline in Europe since EU institution and countries adopted the 5G cybersecurity toolbox in 2020.

When it comes to European security in the cyber realm, we can also observe direct Chinese threats. Recent public cases of cyberattacks against France and the Czech Republic reminded us – again – of cybersecurity challenges from China which was also underlined by the North Atlantic Treaty Organization.

Among other topics, critical technologies, cyber and digital infrastructure top the EU's list of tech security preoccupation with regard to China. This paper provides an analysis of the strategic formulation of EU institutions and European countries on tech security vis-à-vis China from 2013 to 2022. Cases of countries covered in the paper include France, Germany, Greece, the Netherlands, Czech Republic, and the United Kingdom.

The paper is structured as follows. The first part studies the gradual awareness of security implications of Chinese investment in European critical technologies following China's *Made In China 2025* policy. In the second part, the paper examines the security threats posed by Chinese companies' engagement in European digital infrastructure and the coordinated approach of the EU to secure 5G networks. The third part introduces the EU framework for investment screening as a new tool to address security concerns deriving from foreign investment in and acquisition of critical technologies and digital infrastructure. In the fourth part, the paper investigates European cybersecurity agencies and how cybersecurity has become a fast-growing concern of the EU and European countries in its relations with China.

This paper showcases that the European Union and its Member States have incorporated the increasing link between security and technology in their strategic formulation of policy on China. More importantly, the effectiveness of the EU's strategy in tech security highly relies on the coordination and cooperation among Member States and between the EU and national levels.

I. SECURITY OF CRITICAL TECHNOLOGIES

Made In China 2025: The National Policy to Outcompete in Tech

Launched in May 2015, *Made in China 2025* (*MIC 2025*) is China's national policy which aims to upgrade the country's technological and industrial capabilities and to become a high-end manufacturing power in the world by 2049[2]. Chinese government identifies technologies and industries in the fields of information, robotics/ automated machine, aerospace, and new energy vehicles – among other 'key sectors' – in the *MIC 2025* policy[3]. At the core of the policy, the

[1] *This text was originally published by the Observatory of Multilateralism in the Indo-Pacific, Dec 17 2025*

[2] *The year 2049 will mark the centennial anniversary of the establishment of the People's Republic of China (PRC).*

[3] *The State Council of the People's Republic of China. '"Made in China 2025" plan issued.' May 19, 2015.*

goal has been to 'localise' value chains of high-tech industries in China and to decrease China's dependence on foreign high-tech equipment and know-hows.

As a 'signature project' of Chinese President Xi to reach technological advancement *per se*, the *MIC 2025* would not have raised the eyebrows of EU institutions or Member States to such an extent when it reached the end of 2010s. The main reasons that it has been the case lie in China's increased investment in and acquisition of the EU's advanced technologies, and the implications of these Chinese moves on the security of the EU and its Member States. Chinese investment abroad has been very targeted on 'high-tech and advanced manufacturing assets'. These chosen targets are in view of 'clearly defined interests' which are not just economic, but 'overall strategic interests, including the political and security (...) dimension[s].'

Gradual Awareness of Security Implications of Chinese Investment

In the 2013 *EU-China 2020 Strategic Agenda for Cooperation*, the two sides encouraged cooperating on science, technology and innovation, complementing mutual strengths and realising win-win results. In the 2014 *China's Policy Paper on the EU*, China promoted technological exchanges and cooperation with the EU in various strategic emerging industries. These industries include, for instance, renewable energy, digital information, advanced manufacturing, etc. Germany's Federal Ministry of Education and Research, for example, has developed close interactions and cooperation with China[4]. The Chancellery and the Federal Ministry for Economic Affairs held a more positive opinion on economic and industrial engagement with China when some other ministries such as the Federal Foreign Office and the Federal Ministry of Defence presented more cautious attitudes[5]. Former German Chancellor Angela Merkel as well as the Chancellery have focused more on the cooperation aspect in German-Chinese relations[6].

The rosy picture started to change in the *Elements for a new EU strategy on China* in 2016. This EU policy document still encouraged technological and innovation cooperation between the EU and China. However, it stated the growing market access difficulties faced by EU digital tech companies in China following the *MIC 2025* policy and concerns of piracy and thefts of technological intellectual property by China. Moreover, China is also competing with the EU on technological standard-setting in areas such as 5G, artificial intelligence and new electric vehicles[7]. The EU and its Member States gradually started to become more aware of the risks of research and technological cooperation with China. On the Chinese side, its 2018 *China's Policy Paper on the European Union* continued the tone of its 2014 document in promoting cooperation on technology and innovation and did not mention its *MIC 2025* policy or address concerns related to it.

Germany is one of the top industrial powerhouses in the EU and worked well with China as the latter is a huge manufacturing partner. Therefore, the two sides complemented each other. Yet, the situation of Chinese competition with Germany and other Member States in technology-intensive industries has gotten more and more intense and notable since the launch of the *MIC 2025* policy[8]. The Federation of German Industries (BDI) raised the concerns in its policy paper in January 2019. The paper clearly highlighted the *MIC 2025* policy and Chinese actions of state investments in advanced technologies, and 'forced technology transfer and strategic takeovers of foreign high-tech companies' with the aim to achieve 'technological supremacy'. As a result, the BDI referred to China as a 'systemic competitor' aside from a partner.

The reflection and articulation of BDI had a strong influence on referring to China as a 'competitor' and a 'systemic rival' in the EU's *EU-China – A Strategic Outlook* in 2019. This document expressed in an even clearer manner that 'China can no longer be regarded as a developing country. It is a key global actor and leading technological power.' China was, thus, defined as an 'economic competitor in the pursuit of technological leadership' aside from a partner and a systemic rival. The EU pinpointed that China developed its 'strategic high-tech sectors' while limiting market access and demanding forced technology transfers to foreign companies through the *MIC 2025* policy. Moreover, the

[4] *Interview with Friedolin Strack, online, June 2021. Following the gradual awareness of the security risks in research, technology and innovation cooperation with China, the German Federal Government established a cross-ministerial coordination mechanism on Chinese issues in 2018.*

[5] *Interview with an expert on Asia of a German political party foundation, online, June 2021.*

[6] *Interview with an expert on Asia of a German political party foundation, online, June 2021, and interview with a German official, online, June 2021.*

[7] *Interview with an EEAS official, online, May 2021.*

[8] *Interview with Reinhard Bütikofer, online, February 2021.*

document also stated that foreign investment in and acquisition of the EU's critical technologies 'can pose risks to the EU's security'. We can observe that security challenges from foreign investment in and acquisition of critical technologies gradually became a key topic in the EU's policy on China in the second half of the 2010s[9]. The awareness of the EU and its Member States about the link between security and technology was a 'very recent' phenomenon[10].

Germany is a prominent example of increasing vigilance on China's moves of acquiring advanced technologies in the EU. The acquisition of German company *KUKA* by Chinese enterprise *Midea* in 2016 was often labelled as the 'wake-up call' or a 'point of no return'[11]. *KUKA* was a German company leading in the industrial robotics sector around the globe while *Midea* is a Chinese electrical appliance manufacturer specialising in products such as laundry, refrigerating, and air-conditioning appliances. The German government authorised the takeover deal in August 2016, explaining that it will not 'threaten the security' of the country. Stories were covered in the media that the CEO of *KUKA* shared different strategies for the development of the company from the Board Chairperson from the mother company *Midea*, and *KUKA* changed its CEO in December 2018. The takeover deal attracted concerns and debates about the risks of high-end technologies in the EU acquired by foreign companies, especially when a foreign country has developed a national policy to compete in technological advancement.

In another case of the takeover of *Aixtron* by *Fujian Grand Chip Investment Fund*, the deal was stopped by the German government in October 2016. *Aixtron* is a German semiconductor equipment supplier while *Fujian Grand Chip Investment Fund* is a Chinese buyout fund firm. The German Federal Ministry for Economic Affairs initially approved the deal in September 2016 amid concerns and debates similar to the *KUKA* case a month earlier. In October, the Federal Ministry for Economic Affairs re-examined the deal again following 'previously unknown security-related information', and finally withdrew clearance for such a takeover. The US played a role in the *Aixtron* case. The US Committee on Foreign Investment – an interservice committee of the US government chaired by the Treasury Secretary to examine the effects of foreign investment on national security – examined *Aixtron* because the company also holds assets in the US. The US Committee on Foreign Investment raised security alerts to the German government. The *Fujian Grand Chip Investment Fund* finally decided to drop the purchase deal in December 2016.

These two cases are illustrative examples of the increasing link among economic, security and technological dimensions. Germany has had the habit of trying to separate economics on one side and politics and security on the other due to history[12]. Since the launch of the *MIC 2025* policy, 'a shift in Germany's traditionally open investment posture' can be observed following security concerns from Chinese investment in and acquisition of advanced technologies. Chinese investment in German critical technologies have attracted more and more debates and public attention[13]. Germany has become aware of the security implications of foreign investment in critical technologies.

For the Netherlands, China and its investment in advanced technologies had not been on the security radar screen before the second half of the 2010s[14]. The beginning of the 2010s was a moment when the country was undergoing a defence budget cut. Security topics were concentrated on the European continent, or to be more precise, the EU and the Eastern neighbourhood. At the same time, the Netherlands has followed the policies and priorities of NATO closely[15]. NATO started to alert emerging challenges from China in the second half of the 2010s, and officially recognised China as an important topic of the Alliance in its London summit in 2019. The Netherlands has gradually paid attention to Chinese investment in and acquisition of – sometimes even theft – advanced technologies.

Leiden University in the Netherlands terminated its partnership agreement with China's Confucius Institute by the end of August 2019 due to the reason that 'the Confucius Institute's activities no longer align with the University's China strategy'. The decision of the university was an example of the gradual concerns

[9] *Interview with an EEAS official, online, May 2021.*

[10] *Interview with François Godement, Paris, July 2021.*

[11] *Interviews with three German officials, online, June 2021.*

[12] *Interview with an expert on Asia of a German political party foundation, online, June 2021.*

[13] *Interview with a German official, online, June 2021.*

[14] *Interviews with two Dutch officials, online, March and May 2021.*

[15] *Interviews with a Dutch official, online, March 2021.*

about the risks and challenges of scientific cooperation with China – aside from opportunities[16]. Such risks and challenges include, for instance, potential theft of data and intellectual property, 'censorship and infringement of academic freedom', and that Chinese scientific research has aligned more and more with the country's governmental 'security needs and strategic vision'. Moreover, on the security dimension of scientific cooperation, the Dutch security and foreign affairs services have worked on raising the awareness of other governmental and non-governmental institutions which have regarded China as opportunities about the risks and challenges that come with collaboration. These institutions include, for example, businesses, academic establishments, and non-central governments (provinces and municipalities), and the Ministry of Economic Affairs and the Ministry of Education, Culture and Science.

In May 2019, the Netherlands published a policy document *The Netherlands and China: A New Balance* which can be seen as a shift in Dutch policy on China. In the document, China was described as a 'strong competitor' in technology which aims to become a 'technological superpower' through its *MIC 2025* policy. Among other government-led actions, China has imposed forced tech transfers on foreign companies, invested and acquired foreign enterprises, and mobilised 'aggressive digital tactics' to gain access to advanced technologies.

The 2022 annual report of the Netherlands' General Intelligence and Security Service stated that China serves as the 'greatest threat' to the Netherlands' 'economic security' and 'national security interests' – aside from Russia. The reason is that China has been seeking to strategically acquire Dutch and EU advanced technologies. China's attempts include both through legal (such as investment, merger and acquisition, joint research projects) and illegal manners (such as espionage, covert investment, illegal exports).

France also had rising concerns about the link between security and technology in the country's relations with China since the second half of the 2010s[17]. First, the serious preoccupation vis-à-vis Chinese ambition and activities of acquiring intellectual property related to advanced technologies of France and other EU Member States. Second, related measures of China to build restrictions to prevent foreign access to its technological capabilities. On the tech and security aspect, upholding the EU flag is the most suitable approach for France to have enough leverage in the negotiations with China and to avoid threats from China on individual Member States[18].

From this part, we can observe the gradual awareness of the security dimension of critical technologies, through Member States' cases of Germany, the Netherlands and France. Such a progress is rooted from both China's *MIC 2025* policy and increasing concerns on Chinese investment in and acquisition of advanced technologies of Member States. These concerns on risks and challenges from China were also reinforced by the shift in perceptions of the EU and its Member States vis-à-vis China as an 'economic competitor in the pursuit of technological leadership'.

II. SECURITY OF DIGITAL INFRASTRUCTURE

Researchers have written about the phenomenon that critical infrastructure such as ports, airports, railway, and electricity grids on the EU soil is generally 'too open' to foreign acquisition or even ownership through investment. This phenomenon contributes to the risk of foreign actors – public and private – interfering politically and strategically the European Union and its Member States. Security concerns related to the EU's digital infrastructure due to foreign investment and acquisition started to receive more serious attention since the second half of 2010s. Researchers have also underlined the fact that trade and investment have increasingly been linked to tech security, especially in the domain of digital infrastructure[19].

Digital infrastructure refers to 'a set of information and communication technology components that are the foundation of information and communication technology-services. These include typically physical components – computer and networking hardware and facilities – but also various software and network components'.

[16] *Interviews with a Dutch official, online, March 2021.*

[17] *Interviews with two French officials, Paris, June and August 2021.*

[18] *Ibid.*

[19] *Interview with Gudrun Wacker, online, June 2021.*

The topic of digital infrastructure neither appeared in the 2013 *EU-China 2020 Strategic Agenda for Cooperation*, nor in *China's Policy Paper on the European Union* in 2014. The European Union's concerns started to emerge in its *Elements for a new EU strategy on China* in 2016. The EU expressed its discontent on China's security reviews of EU investment in China beyond 'legitimate national security concerns'. The other way around, the EU stated the need to define the area of critical infrastructure among Member States in the face of China's foreign investment in the EU. The *China's Policy Paper on the European Union* in 2018 did not touch upon the issue of critical infrastructure. However, put under the section of trade and investment, the Chinese document aspired that 'the EU will keep its investment market open'.

The EU's concerns about the security of critical digital infrastructure became concrete and serious in the *EU-China – A Strategic Outlook* in 2019. This policy document dedicated two action plans (Action Nine and Action Ten) to this topic, including one that focused on critical digital infrastructure. The document explicitly stated that foreign investment in and acquisitions of critical infrastructure can put the EU's security under risk. Action Nine mainly concerns the need to safeguard the security of digital infrastructure with a focus on the importance of 5G networks. Moreover, in Action Ten, the policy document stated the need to detect and raise awareness of security threats originating from foreign investment in and acquisition of the EU's critical infrastructure.

At the EU level, digital infrastructure particularly on 5G networks is one top subject that the EU has been working on increasing its leverage when facing China[20]. The EU has put a lot of effort into coordinating national risk assessments and coming up with common EU measures to mitigate security risks of 5G networks. The EU toolbox for cybersecurity of 5G networks includes, for instance, putting in place measures to respond to security risks posed by 5G providers (including dependency reduction, restrictions and even exclusions on high-risk operators), diversifying the supply chain of 5G networks, coordinating among Member States on an EU security certification on 5G infrastructure, and updating reviews of the EU and its Member States on security risks of 5G infrastructure through the NIS Cooperation Group.

Thus, even though there is not yet a common EU 5G policy, there has been concrete progress on establishing Member States' 5G policies and an increase in coherence among national policies on the security of 5G infrastructure. Moreover, despite the fact that Member States are still the final decision-makers of national 5G policies, an EU-wide coordination and cooperation mechanism provides 'positive peer pressure' on Member States' introduction of measures to strengthen the EU's security of 5G networks collectively[21]. As it concerns EU institutions, the ENISA and DG CONNECT have formed task forces to follow and respond to 5G security risks in collaboration with Member States' authorities[22].

The European Parliament has also been active in raising the awareness of security threats from China's engagement in digital infrastructure such as 5G networks of the EU and its Member States. For some Members of the European Parliament, high-risk Chinese telecommunications providers are systematically sensitive for the digital security of the EU and its Member States[23]. In March 2019, the European Parliament adopted a resolution on the topic. The resolution expressed concerns on the vulnerabilities of the European Union's 5G infrastructure constructed by companies of high security risks, called upon incorporating security risks in the analyses of critical infrastructure networks as well as enhancing the coordination among Member States and between EU and national levels. The main plea of the resolution can be found later in the ENISA's *Report on EU coordinated risk assessment of 5G* in October 2019 and the EU toolbox to secure 5G networks in January 2020.

However, the security of digital infrastructure involves Member States' competence especially when related to national security. The European Parliament is able to create debates, raise awareness, and call on the Council, Commission and Member States to make more concrete progress regarding the topic. However,

[20] *Interview with Zaki Laïdi, online, February 2021.*

[21] *Ibid.*

[22] *Interview with an EEAS official, online, May 2021.*

[23] *Interview with Michael Gahler, online, June 2021.*

it is not able to 'force' other actors in the decision-making process regarding this topic[24].

At the national level, France, the Netherlands and the Czech Republic were leading contributors to the EU's 5G security toolbox. France has taken the security of 5G networks seriously, including the need to decrease dependency on Chinese 5G infrastructure's supply chain arrangement[25]. France has been more and more aware of the strategic interests to be protected and security threats posed by foreign investment when it comes to digital infrastructure[26]. In response to such security challenges, France urges that the country and the EU need to set up and mobilise tools at their disposal[27] such as the foreign direct investment (FDI) screening mechanism which will be introduced in the next part. Moreover, the French Parliament passed a law on securing defence and national security interests in the domain of mobile networks (commonly known as the '5G Law') in August 2019. The law requires the operation of specific electronic devices to be authorised by French authorities in charge, and operators need to comply with administrative requirements demanded in the law. In July 2020, the French Cybersecurity Agency informed telecommunication operators that the agency will not renew the authorisation licence to *Huawei* 5G equipment which will expire between three (2023) to eight years (2028).

For Germany, in response to security risks related to telecommunications, the country has been working on building up its resilience of digital infrastructure[28]. With its *IT Security Act 1.0* coming into effect since July 2015, Germany aims to secure its IT system and digital infrastructure. The *IT Security Act 2.0* came into force in May 2021. The German IT security laws require telecommunication operators to meet 'high-level security requirements' and 'critical components' required security certification. German companies in sensitive sectors and 'particularly high economic importance' are demanded to implement IT security measures as well. In September 2023, the German Federal Ministry of the Interior announced the proposal to restrict German telecom operators from using 5G equipment of *Huawei* and *ZTE* by 2026.

Czech officials have noticed that certain Chinese telecommunication enterprises such as *Huawei* and *ZTE* are linked to the activities and interests of Chinese government[29]. Discussions on China's engagement in 5G infrastructure have increased with growing security concerns in the Czech Republic. The Czech National Cyber and Information Security Agency (NÚKIB) issued a warning that software and hardware of *Huawei* and *ZTE* pose threats to Czech cybersecurity. Labelled as the highest threat level 4, *Huawei*'s participation in Czech 5G networks is restricted. Intensified Chinese espionage activities[30] in the Czech Republic also became a topic that the Czech intelligence services watch closely.

The UK has had the first *Huawei* office on its soil since 2001 ahead of other EU Member States. *Huawei* has increased its involvement in British digital infrastructure since 2005. The year was the moment when *Huawei* got contracts from *British Telecom* to upgrade the latter's telecommunication networks, particularly 'routers and other transmission equipment'. The UK's security concerns about the growing engagement of *Huawei* in the country's digital infrastructure started in 2010[31]. Concerns have gotten even more serious since June 2013 when the Intelligence and Security Committee of Parliament – a joint committee of the House of Commons and the House of Lords – published a report on risks to national security posed by *Huawei*'s engagement in the UK's critical digital infrastructure. Responding to the report, the British government acknowledged that the procedures of evaluating the security dimension of *British Telecom*'s contracts to *Huawei* were 'insufficiently robust', agreed that the National Security Adviser will review the functioning of the Huawei Cyber Security Evaluation Centre[32], and recognised the need to adopt a 'risk-based approach' to review foreign investment in the UK's critical infrastructure. After the peak of UK-China relations under David Cameron's prime ministership, the UK's National Cyber Security Centre was established in October 2016 and has also watched closely the security risks of *Huawei*'s equipment and technologies in the UK's digital infrastructure[33]. In July 2020, the UK announced its ban for *Huawei* and

[24] *Interview with Michael Gahler, online, June 2021.*

[25] *Interview with a French official, Paris, June 2021.*

[26] *Interview with François Godement, Paris, July 2021.*

[27] *Interview with a French official, Paris, July 2021.*

[28] *Interview with two German officials, online, June 2021.*

[29] *Interview with a Czech official, online, May 2021.*

[30] *Interview with a Czech official, online, May 2021.*

[31] *Interview with two British officials, online, March 2022.*

[32] *It was set up in 2010 to examine security risks originating from Huawei's increasing presence in the UK's critical digital infrastructure.*

[33] *Interview with two British officials, online, March 2022.*

other of China's high security risk companies from British 5G networks by the end of 2027.

As it concerns Greece, it is interesting to notice the relatively limited presence of China in Greek 5G telecommunication networks. The reason is that China had significantly engaged in Greece's 4G networks since *Huawei*'s investment in upgrading Greek telecommunication company *Wind Hellas*' 4G networks amidst the severe hit of the financial crisis. *Huawei* is reported to account for more than 50% of Greece's radio access network which is the telecommunication component connecting individual devices to other parts of telecommunication networks. *Wind Hellas*' radio access network is almost exclusively provided by *Huawei*. However, when gradually moving onto 5G infrastructure, at the end of 2010s and even more since 2020, Greece met the moment when the US and other EU Member States started to discuss or prohibit the participation of *Huawei* and *ZTE* in 5G infrastructure on their soil. In June 2020, Greece joined the Clean Network initiative promoting the ban of digital equipment and services from authoritarian governments. Even though Greece has not decided to prohibit *Huawei* from taking part in Greek 5G infrastructure, the country has distanced itself from the company.

We can notice a similar trend as the topic of cybersecurity. The EU and its Member States have been increasingly noticing and reacting to the security concerns posed by Chinese engagement in digital infrastructure – starting with 5G – on the EU soil. The EU has been pushing for Member States's progress on establishing national 5G security policies. Member States are more and more aware of the security risks of Chinese companies providing 5G equipment and services. To a different extent, Member States have been adjusting their 5G regulations regarding Chinese high-risk enterprises, especially the case of *Huawei* and *ZTE*.

III. THE NEW TOOL TO RESPOND: EU FRAMEWORK FOR FDI SCREENING

The EU's new tool to address security concerns deriving from foreign investment in and acquisition of critical technologies and infrastructure is the FDI screening mechanism. The mechanism constructed a framework, on the one hand, for Member States to scrutinise FDI on the basis of security or public order, and on the other hand, for coordination and cooperation among Member States and between the EU level and the national level.

The Commission presented the proposal of the EU framework for FDI screening in September 2017. The Council and the European Parliament reached a political agreement on the mechanism in November 2018. In March 2019, the FDI screening mechanism was adopted. In fact, the FDI screening mechanism was based on the initiation of France, Germany and Italy in February 2017[34]. Even earlier back in May 2012, the European Parliament had already adopted a resolution which called on the set-up of 'a new institutional framework' to tackle the security implications of foreign strategic investment with reference to the design of the US Committee on Foreign Investment.

The EU framework for FDI screening was seen as an important milestone for the EU and its Member States for two main reasons[35]. First, the mechanism was set up within eighteen months which is a very efficient timeline for the EU's decision-making. Consensus was found in a relatively short span of time despite being a novel concept. The consensus on the need for this new tool was found in the EU ecosystem based on analytical work conducted by Member States and EU institutions. Second, the EU is able to mobilise the competence on trade and investment, and link it to security issues which opened up new dimensions of the field of security.

It is important to underline that reviews and the final say on foreign investment cases are carried out by Member States based on their national screening mechanisms with variations in scope and criteria. That being said, EU framework for FDI screening allows coordination of these reviews at the EU level. For instance, the Commission can issue opinions on cases of foreign investment, Member States have the obligation to notify the Commission about screened FDI cases, Member States are called upon to update and set up national screening mechanisms, and contact points of the Commission and of Member

[34] *Interviews with a German official and with Mikko Huotari, online, June 2021.*

[35] *Interview with a Commission official, online, February 2021.*

States were established to exchange information. FDI is a topic under the exclusive competence of the EU while the issue of national security is a Member State competence. Therefore, the effectiveness of the EU framework for FDI screening heavily depends on the coordination and cooperation between the EU level and the national level.

Primary materials through interviews showed praises from researchers and policy-makers to the EU framework for FDI screening as a concrete and useful tool of the EU in the face of security challenges derived from foreign investment in and acquisition of the EU's critical technologies and infrastructure[36]. With this tool at its disposal, the EU increased its leverage when interacting with China. The mechanism bears the core belief that the EU remains open to foreign investment, but it must also protect its critical technologies and infrastructure if there are security implications.

IV. CYBERSECURITY

Cybersecurity Authorities in the EU

In its Cybersecurity Act in 2019, the European Union (EU) defined 'cybersecurity' as 'the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats'. The European Union generally mobilised the terminology of 'security of network and information (systems)' instead of 'cybersecurity' in its legal documents before the *Cybersecurity Act*.

In terms of the authorities of the EU and Member States responsible for cybersecurity, the body at the EU level in charge is the European Union Agency for Cybersecurity (ENISA). The ENISA was established under the name 'European Network and Information Security Agency' in March 2004. The aim of the agency is to 'assist the Commission and the Member States, and in consequence cooperate with the business community, in order to help them to meet the requirements of network and information security'. It was explicitly expressed in the regulation which founded the ENISA that the functioning of the ENISA 'shall be without prejudice to' Member States' competences. This reminds us the importance to include the national level in the study of this topic. The ENISA's mandate – in terms of duration – was extended in 2008, 2011, and 2013 before becoming a permanent European Union agency under its current name 'European Union Agency for Cybersecurity' in 2019.

At the national level, legal frameworks and structures of national cybersecurity authorities vary greatly[37]. For instance, for the six selected countries studied in this paper, the French Cybersecurity Agency (ANSSI) was created among the earliest in 2009, and is supervised by the General Secretariat for Defence and National Security (SGDSN) under the Prime Minister's authority. Germany's National Cyber Response Centre (Cyber-AZ) was established in 2011. It is not an authority itself but performs services in the Federal Office for Information Security (BSI) under the Federal Ministry of Interior (BMI). As it concerns the Czech Republic, the country set up its National Cyber and Information Security Agency (NÚKIB) in 2017 replacing both the National Cyber Security Centre (NCKB) and the Cyber Security Council (CSC) established in 2011. The NÚKIB is under the authority of the Prime Minister whom the NÚKIB chief reports to. The Dutch National Cyber Security Centre (NCSC-NL) was set up in 2012, and is under the Ministry of Justice and Security (JenV). Established in 2016, the UK's National Cyber Security Centre (NCSC) is under the Government Communications Headquarters (GCHQ). The GCHQ is not part of the Foreign, Commonwealth & Development Office (FCDO), but is under the supervision of the Foreign Secretary. For Greece, the country had its General Directorate for Cybersecurity under the Ministry of Digital Governance which was set up in 2019. The Greek government established the new agency National Cyber Security Authority in 2024 and remains under the supervision of the Minister of Digital Governance.

In order to facilitate the coordination and cooperation between the EU and its Member States on cybersecurity, the Network and Information Systems (NIS) Cooperation Group has been established since July 2016. The NIS Cooperation Group gathers the Commission, the ENISA, and representatives of national cybersecurity authorities of Member States.

[36] *Interviews with Zaki Laïdi, online, February 2021, with a Czech official, online, May, 2021, with a Dutch official, online, May 2021, with three German officials, online, June 2021, with Mikko Huotari, online, June 2021, with three French officials, Paris, June, July, and August 2021, and with an EEAS official, online, July 2021.*

[37] *Interview with a Czech official, online, May 2021.; Vincent Strubel, 'Quelle stratégie pour la France face à une menace cyber en pleine croissance ?' Speech at Sciences Po, Paris, 6 March 2024.*

The EU directive which set up the NIS Cooperation Group aims to ameliorate coherence of the EU by demanding Member States to assign a national service as well as a single contact point in charge of cybersecurity. The NIS Cooperation Group also aims to enhance exchanges among Member States on information concerning cybersecurity. At the same time, the directive underlines the respect of Member States' competence in determining the disclosure of information in view of national security. Interviews with practitioners of Member States showed that that there has indeed been resistance from certain Member States to an EU-level cybersecurity authority[38]. After all, as an EU directive, although being a legally binding act, it is the Member States which adopt the national laws on how to realise the goals put forward by the directive – or 'transposition'[39] in EU legal language.

Cybersecurity in EU-China Relations

In European Union-China relations, cybersecurity was already mentioned as a concern in the EU's policy document *EU-China 2020 Strategic Agenda for Cooperation* in 2013. The prospect of enhancing trust and cooperation between the two sides in the cyber domain under the UN framework was present. The *China's Policy Paper on the EU* in 2014 basically stated the same content as in the EU's document in 2013.

The EU's *Elements for a new EU strategy on China* document in 2016 began to indicate the EU's concerns about China's 'cyber-enabled theft of intellectual property rights and trade secrets'. The EU also urged China to 'apply existing international law in cyberspace', and to jointly promote an international agreement on 'protecting critical cyber assets'. In 2018, Chinese expressions regarding cybersecurity in its *China's Policy Paper on the European Union* were only a paraphrase of its policy paper in 2014.

The *EU-China – A Strategic Outlook* document in 2019 addressed the issue of cybersecurity under one of the ten action plans. It is to enhance the security of critical digital infrastructure of the European Union and its Member States. It can thus be understood that cybersecurity was listed as one of the European Union's top priorities in its relations with China. Moreover, the EU's 2019 policy document also signalled the seriousness of the European Union and its Member States on cybersecurity by indicating the EU's progress on setting up a framework for sanctions regime against cyber-attacks. In May 2019, the EU Council adopted a regulation to establish such a sanctions framework allowing the European Union to impose sanctions (travel bans and asset freezes) on 'persons or entities that are responsible for cyber-attacks or attempted cyber-attacks'. We can, therefore, observe a trend of growing concerns from the European Union and its Member States on the security of the cyber domain in their relations with China.

Ten days after the publication of the policy document on China in 2019, the European Council invited the European Commission to propose a recommendation on a 'concerted approach' to the EU's cybersecurity of 5G networks. Four days later, the European Commission put forward its recommendation. The Commission's recommendation calls upon Member States to conduct national 5G risk assessments and take security measures needed in response to the risk, and to develop a coordinated risk assessment and common mitigation measures at the EU level jointly with EU institutions and Member States. In October 2019, through the NIS Cooperation Group, the *Report on EU coordinated risk assessment of 5G* was published. In January 2020, the NIS Cooperation Group adopted an EU toolbox of mitigating measures for cybersecurity of 5G networks aiming to respond to 5G cybersecurity challenges collectively.

For the case of the Czech Republic, the country has been one of the active contributors to the EU's cybersecurity policy. As a Czech official put it vividly, cybersecurity is a 'disaster-driven' topic that Member States know is critical but usually do not do much concretely or work together with other EU capitals before negative incidents happen[40]. When starting to be interested in enhancing interactions with Central and Eastern European countries in the first half of 2010s, China did not have much knowledge about

[38] *Interview with a Czech official, online, May 2021.*

[39] *Article 288 of the Treaty on the Functioning of the European Union.*

[40] *Interview with a Czech official, online, May 2021.*

or presence in the region before. Intelligence has been an important source of acquiring information to provide policy guidance for China regarding the region. The Czech Republic began to detect cyber espionage activities that were able to be attributed to China around 2013 and 2014[41]. Echoing the concerns mentioned previously in the EU's policy documents on China, cyber infringements have also been observed in thefts of intellectual property rights of European enterprises. Related Czech governmental services have, thus, started to closely watch China's cyber activities vis-à-vis the country.

Germany has also addressed cybersecurity concerns coming from foreign threat actors[42], including China which has become a 'major source of cyberattacks against Europe' with an aim to implement its 'ambitious industrial policy'. Or as German officials framed it, China 'is clearly concerned' when it comes to cyber-attacks[43]. In December 2019, Germany's Federal Office for the Protection of the Constitution (BfV) published a report related to cyber-attacks attributed to the *Winnti Group*, a Chinese hacking group allegedly state-sponsored. The report indicated cases such as *Winnti Group*'s attacks on German enterprises *Henkel* (2014), *BASF* (2015), *Siemens* (2016), *Bayer* (2018), and *Roche* (2019) among others. Researchers depict that such attacks targeted German tech and pharmaceutical companies and also gradually German governmental entities and diplomatic missions abroad from 2022. The percentage of German companies which reported to have encountered China's cyber infringements rose from 30 in 2021 to 43 in 2022.

From this section, we observe a fast-growing attention of the European Union and its Member States to cybersecurity in their relations with China since 2013. Even though China is surely not the only, it is clearly one of the main countries of cyber infringements against EU institutions and Member States. EU actors – although very different in terms of their legal structures – have established agencies in charge of cybersecurity as well as a coordinating body between the EU and its Member States. The core difficulty for the EU's coordination and cooperation regarding cybersecurity lies in the fact that Member States' competence prevails when national security is concerned. With the EU toolbox for 5G cybersecurity adopted in January 2020, it provides a framework for EU institutions and Member States to mitigate 5G cybersecurity challenges collectively.

***

The security in tech, cyber and digital infrastructure has not really emerged as a subject in EU-China relations in 2013. Since the second half of the 2010s, it has become a more and more serious preoccupation of EU institutions and Member States.

While the *MIC 2025* policy aspires to upgrade China's technological and industrial capabilities, the country's investment abroad has been very targeted on high-tech and advanced manufacturing assets. The EU and its Member States have increasingly realised the need to secure their critical technologies in the face of Chinese investment and acquisition. On cybersecurity, China has increasingly been identified as a major source of attacks against the EU and its Member States. On digital infrastructure, EU actors have come to be on their guard against security challenges posed by Chinese engagement in digital infrastructure, starting with 5G.

In collaboration with Member States, the European Union adopted the EU framework for FDI screening in March 2019. The mechanism created an EU-level framework for the Commission and Member States to coordinate actions regarding FDI. It is the EU's new tool to review and moderate China's increased investment in and acquisition of Europe's critical technologies and infrastructure on the grounds of security or public order. The European Union and its Member States set up this tool in a very efficient manner, and mobilised the EU competence on trade and investment to link it to the security domain.

This paper showcases that the European Union and its Member States have incorporated the increasing link between security and technology in their strategic formulation of policy on China. EU actors started from noticing, to increasingly being vigilant, and to setting

[41] *Ibid.*

[42] *Interview with two German officials, online, June 2021.*

[43] *Interview with two German officials, online, June 2021.*

up measures to respond to challenges to Europe's tech security in their interactions with China. Tech security has been significant in the strategic formulation of EU policy on China.

Aside from the endeavours of EU institutions, Member States have played a significant role in the process of this strategic formulation as national security concerns the competence of Member States. The effectiveness of the EU's strategy in tech security highly relies on the coordination and cooperation among Member States and between the EU and national levels. In this regard, the EU toolbox for 5G cybersecurity, the EU sanction regime against cyberattacks, and the EU framework for FDI screening can be deemed as concrete achievements. However, the actual implementation of tech security measures vis-à-vis China by Member States remains the key homework for a well-formulated EU strategy to be successful.

Dr Earl Wang

Associate researcher and lecturer at the Centre for International Studies (CERI) - Sciences Po/CNRS

Directeur de la publication : Pascale JOANNIN
ISSN 2402-614X