EU-CHINA OBSERVER

DEPARTMENT OF EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES

College of Europe
Collège d'Europe
DEPARTMENT OF EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES

Baillet Latour Chair of
European Union-China Relations

College of Europe
Collège d'Europe
EU-CHINA Research Centre
EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES
BAILLET LATOUR FUND

4.19

TABLE OF CONTENTS

COLOPHON

Baillet Latour Chair of EU-China Relations / EU-China Research Centre
Department of EU International Relations and Diplomacy Studies, College of Europe, Dijver 11, BE-8000 Bruges, **www.coleurope.eu**

Views expressed in the EU-China Observer are those of the authors only and do not necessarily reflect positions of either the editors or the College of Europe.

ISSN 2506-8415

Professor Jing MEN
jing.men@coleurope.eu
+32 50 477 258

Michele CASADEI
michele.casadei@coleurope.eu
+32 50 477 257

EU-China Observer Inbox
EUCO@coleurope.eu

College of Europe
Collège d'Europe
Brugge
Natolin

DEPARTMENT OF **EU INTERNATIONAL RELATIONS** AND **DIPLOMACY STUDIES**

Baillet Latour Chair of
European Union-China Relations

College of Europe
Collège d'Europe
Brugge
Natolin

EU-CHINA Research Centre
EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES
BAILLET LATOUR FUND

ABOUT THE EU-CHINA OBSERVER

The electronic journal **EU-China Observer** is jointly published by the **Baillet Latour Chair of European Union-China Relations** and the **EU-China Research Centre** based in the Department of EU International Relations and Diplomacy Studies at the College of Europe in Bruges. The journal provides a platform for scholars and practitioners to further deepen the academic analysis and understanding of the development of EU-China relations from an interdisciplinary perspective.

The **EU-China Observer** publishes scholarly articles based on theoretical reasoning and advanced empirical research, practical policy-oriented contributions from all fields of EU-China relations, and conference reports on the annual conferences organised by the Baillet Latour Chair and the EU-China Research Centre. The journal targets academic audiences as well as policy practitioners, members of the business community, NGO representatives, journalists and other interested persons.

BAILLET LATOUR CHAIR / EU-CHINA RESEARCH CENTRE

With the financial support of the Baillet Latour Fund, the College of Europe established in 2008 the Baillet Latour Chair of European Union-China Relations and in 2014 the EU-China Research Centre. The **Baillet Latour Chair of European Union-China Relations** offers courses on EU-China relations at the College of Europe in both Bruges and Natolin. It also organises guest lectures, international conferences and promotes multidisciplinary research on the European Union's relations with China. At the end of each academic year, the Chair grants an award for the best Master's thesis on EU-China relations.

www.coleurope.eu/EUChinaChair

The **EU-China Research Centre** follows closely the development of the European Union-China relationship and its three institutional pillars: political dialogue, economic and sectoral dialogue, and people-to-people dialogue.

The Centre's research focuses in particular on economic questions such as China's New Silk Road initiative and its impact on EU-China relations, the negotiation of an EU-China investment agreement as well as the EU's and China's international influence, especially in Asia and Africa. More generally, the Centre seeks to

- undertake high quality research, preferably from an interdisciplinary perspective, on topics of major importance in the field of EU-China relations;
- publish the research results with well-known publishing houses and in reputable academic journals;
- develop cooperation and exchanges with universities and scholars who are specialised in EU-China studies;
- organise conferences, mainly in Bruges and Brussels; and
- host visiting scholars working on EU-China relations.

www.coleurope.eu/EUChinaCentre

Scholars and practitioners interested in contributing to the **EU-China Observer** should refer to the instructions on www.coleurope.eu/EUCO.

Prof. Jing MEN
Director of the EU-China Research Centre and Baillet Latour Professor of European Union-China Relations

College of Europe Collège d'Europe
DEPARTMENT OF EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES
Baillet Latour Chair of European Union-China Relations

College of Europe Collège d'Europe
EU-CHINA Research Centre
EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES
BAILLET LATOUR FUND

HOW THE FOURTH TECHNOLOGICAL REVOLUTION IS SHAPING THE EU'S VIEW OF CHINA

FRANCESCA GHIRETTI

Introduction

Industrial and technological revolutions are moments of disruption which by changing the ways of production, change society and how we live. Technological revolutions also bring change to global dynamics; they have an impact on the power balances and the way states interact with one another. This article focuses on the changes the unfolding fourth industrial revolution has brought to the relationship between China and the EU, in particular, how the way in which the EU views and responds to China has taken a negative turn.

The literature available on the relationship between the EU and China is vast, as it is the set of academic works on the European perception of China. Despite this, as argued by Richard Maher,[1] more systematic analysis is needed, especially with respect to the strategic responses of the EU to China. However, in order to be able to provide effective strategic responses, we first must understand the reasons behind the most recent views the EU has of China.

The image the EU has been constructing of China has changed multiple times since what it is often pinpointed as the beginning of their relationship, 1975.[2,3] Such changes cannot be merely attributed to a modification of views entirely unrooted from the material condition in which the two are embedded; great changes such as the economic rise of China, as well as lack of expected changes in China's political system have contributed to the mutation of the EU's view of China.

This article, however, argues that most recent changes in the way the EU views China are mainly due to the variations brought about by the fourth technological revolution. This recent EU view of China has been characterised by a negative turn. History has been witness to numerous industrial and technological revolutions, which are periods characterised by a significant change in the manners of production and consequently in the ways of life of societies which are directly and indirectly touched by it. The fourth industrial revolution, specifically, concerns the development of a smart type of technology. Several scholars have argued that as far as previous industrial revolutions are considered the country which led such a process was then able to secure its supremacy and advantageous position over the other countries.[4,5] As these revolutions have always taken place in the West, whether in England, Germany or the US, the West has so far been granted a preferential position in the working of the global dynamics and in shaping its rules.

The fourth industrial revolution, which is now unfolding, however, is making China a realistic candidate for the role of leading country in the development of smart technologies; thus, shifting the locus from the West to the East. It is thus argued here that the material changes potentially brought by this smart revolution, which is yet to be completed, have had a great influence on the way the EU, the former holder of such primacy whether directly or as part of the West, views China as a competitor for industrial leadership.

First, it will be shown that the way in which the EU views China has taken a negative turn by highlighting three decisive turning points that have been identified: the 2016 EU Global Strategy, the 2017 proposal for a pan-EU screening mechanism for foreign direct investments (FDI), the 2019 EU-China Strategic Outlook. Then, it will be argued that these changes are rooted in the technological revolution and the implications this has in shaping future global dynamics, based on these four recent developments: the realisation of the decreasing level of complementarity of the Chinese and European economies, the adoption of a pan-European screening mechanism for FDI, a growing push for European champions and the hostility towards the development of the 5G network by Huawei.

Changing views – A negative turn

In 2016, the EU's 2016 Global Strategy included a series of requisites to be fulfilled.[6] The document explicitly mentions difficult issues such as the respect of the rule of law, human rights and intellectual property rights (IPR) as fundamentals for the future development of the relationship with China. In regard to IPR, high-end technology is explicitly cited, signalling an existing European concern for China's unlawful practices and the potential disadvantage such practice could bring to the EU.

The subsequent year, 2017, the European Commission, following the initiative of France, Germany and Italy, initiated the legal procedure for the adoption of the EU screening mechanism for FDI.[7] The mechanism was aimed at the screening investments considered to be a risk for the security of the EU. Although it was not explicitly targeting FDI from China, the timing of the proposal and its subsequent adoption, plus the content of the legal text implicitly but unmistakably point at investments originating from China. Its adoption signalled a European decision to counterbalance the political-economic involvement of China in the region.[8]

A more clear-cut and assertive negative turn, however, did not take place until 2019, when the EU-China Strategic Outlook was released and described China as a "systemic rival" and "economic competitor".[9] Other examples of worsening evaluation vis à vis China can be found, however these three clearly show the progressive deterioration of the EU's view of China.

The role of the technological revolution

Why has the European view towards China become increasingly negative? The reasons provided by different scholars have been numerous and are widely debated.[10] This paper argues that the fourth industrial revolution and its implications for the future global dynamics plays a central role in such turn.

First, the EU realised that what was once considered to be a complementary economy is becoming not only a competitor, but also one that does not necessarily follow the same rules and thus, is difficult to deal with.[11] Pepermans notices that "the EU will import labour-intensive products from China and export capital-intensive goods to China" is faulted.[12] However, the wording of the 2019 EU-China Strategic Outlook shows that the EU worries that the more the Chinese economy grows in complexity and in size the more China will compete with and eventually replace the European economy.[13] Should the technological revolution see China leading sectors in which the EU currently competes, then the EU will risk being marginalised on the global scene, both economically and politically.

Second, various analyses have already been provided which attempt to explain the wary attitude of Brussels towards Chinese investments.[14] Of all the factors presented in these works, the asset-seeking nature of Chinese FDI is here deemed to be the most relevant.

THE FOURTH INDUSTRIAL REVOLUTION, WHICH IS NOW UNFOLDING, HOWEVER, IS MAKING CHINA A REALISTIC CANDIDATE FOR THE ROLE OF LEADING COUNTRY IN THE DEVELOPMENT OF SMART TECHNOLOGIES.

That Chinese investments are driven to the EU by asset-seeking motives is broadly agreed upon. However, it is unclear whether these FDI are aimed at exploring European assets or at exploiting them. Recent studies have concluded that if at the beginning Chinese investments might have been driven to Europe by asset exploration, the current situation sees these investments as predominantly exploitative.[15] The main concern thus, is that innovative and strategic technological know-how obtained in Europe is then transferred in China and used to further develop Chinese firms and China's technological advancement,

thus contributing to China's ability to lead the fourth technological revolution and the subsequent marginalisation of the EU.[16] While Europe risks seeing its technological advantage disappear, China becomes stronger and richer.[17]

Thirdly, there is a growing push for European champions, mainly driven by France and Germany but which receives increasing support.[18] It must be, however, acknowledged that in this case another factor also plays a major role; the decision of the US, under the presidency of Donald J. Trump, to distance itself from the EU as preferred ally and partner.

Concerns regarding China taking the lead in the fourth technological revolution has also pushed European countries to advocate for European champions. In fact, numerous major Chinese enterprises are state-owned; in the West, this is often perceived as unfair competition. Thus, Chinese enterprises receive governmental support which makes them more competitive and stronger, while smaller European private enterprises struggle. Consequently, EU states, which do not adopt such supporting mechanisms, are trying to find ways to shift their enterprises out of such a disadvantaged position in order not to be side lined by China. The growth of Chinese big multinational, whether state-owned or private, has led to the perception of the necessity to advocate for support of EU champions.[19]

More specifically, moreover, the actions of state-owned enterprises are often viewed as strongly connected with the will of the state they originate from. This view further increases the perception that there is a planned political-economic strategy behind the actions of these enterprises. However, this evaluation is often then attributed to Chinese private enterprises too.[20]

Fourth, the EU has been expressing concerns in regard to the development by Huawei of the 5G network in its members, which recently culminated in the publication of the EU-wide coordinated risk assessment of 5G networks security. 5G, together with the development of artificial intelligence (AI), is considered to be one of the cornerstones of the fourth industrial revolution and thus, fundamental for the development of a more connected and smart society. This means that developing 5G in a country could potentially empower the developer and provider of such network with an unknown degree of leverage over such society. Moreover, despite Huawei having declared otherwise, the EU still views it linked to the Chinese government. To give such (potential) power over the future of the European society to China presents a risk which many are not willing to take.

The case of Huawei arguably offers us a preview of a possible future in which the technological advancement of China has surpassed that of the EU. In this scenario, the EU might find itself in the difficult position of either accepting China's terms or lagging behind. Given the fact that the matter is still unfolding, and changes occur at an unprecedented speed, more research is needed to better understand the actual security risks posed by Huawei and states have been already moving in this direction. An increasing number of European countries have been placing Huawei under enhanced scrutiny and at times, concluding that allowing the Chinese telecom giant to develop the 5G network presents security risks.

Despite the security concerns and the broader worries linked to the technological revolution and the implication this might bring to the role of the EU in the world, the European response has been a mix of assertive and hopeful statements, which show both the persistent inability of the EU to take a united position and at the same time, its reticence in damaging its relationship with China. This ambiguity, however, strengthens rather than hinders the argument presented here. Although the EU is wary that it would be marginalised by China's rising leadership in the fourth industrial revolution, the EU is also aware of the risks posed by excessively hurting its relationship with China. Such risks are not only linked to the current economic benefits China brings to Europe, but also to the potential future benefits such relationship might give; as well as the risks that severing the relationship with a potential future economic global leader might bring.

Conclusion

This paper has argued that recently, the negative responses the EU has been giving to China are driven by the view that the technological advancement of China will make it capable of leading the unfolding technological revolution and potentially, marginalising the EU as an economic and political actor. Among other factors, this technological advancement is viewed as being strengthened by a transfer of know-how from the EU to China and by the inability of European enterprises to compete with Chinese counterparts. Such a situation has contributed to the emergence of China as leader of the fourth technological revolution and thus, of the system that might result from it.

Despite the existence of such concerns and the role played by it in informing the most recent negative trend in EU responses towards China, generally, the EU's position towards China cannot be described as negative. It is here argued that among other reasons, this is due to the consid-

eration that on top of the existing economic contributions China brings to the EU's economy, in the future, China might occupy an even more important global role. This consideration is informing the EU decision to play it safe in order to avoid being further marginalised or excluded.

Given the current global climate and the non-aggressive nature of the EU, arguably, such approach is a good starting point to avoid premature and unnecessary clashes with China. However, this initial positioning must be further developed into an appropriate yet flexible strategy. First, the EU should understand and make clear what it wants from its relationship with China. Then, work out an approach which would avoid both the undermining of EU's values and an excessively ideological positioning. The EU should thus keep external pressure at bay and consider its own interests in making decisions, to be able to do so it needs to become more independent and reliant on its forces and assets. The cornerstone to the achievement of such independence is the growth of investments, both in terms of money and energy, in favour of European champions, starting from the sectors in which the EU already occupies a leading position. Then, increase investments in research and development through which the EU can increase its know-how and place itself in an advantageous position vis à vis current and future technological revolutions. ©

1 R. Maher, "Europe's response to China's rise: competing strategic visions", Asia Europe Journal, Vol 15, no. 2, 2017, pp. 133-145 **2** D. Scott, "China-EU convergence 1957–2003: towards a 'strategic partnership'", Asia Europe Journal, Vol 5, no. 2, 2007, pp. 217-233 **3** J. Men, "The EU and China: mismatched partners?", Journal Of Contemporary China, Vol 21, no. 74, 2012, pp. 333-349 **4** R. O'Brien & M. William, Global Political Economy. Evolutions and Dynamics, Red Globe Press, 2016, 5th edn. **5** P. Kennedy, The rise and fall of the great powers, Vintage Books, 1989 **6** European Union, "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy", June 2016, p. 38 **7** "Screening of foreign direct investments", European Commission, 24 June 2019, retrieved 4 January 2020, https://trade.ec.europa.eu/doclib/press/index.cfm?id=2006. **8** F. Van der Putten, "Chinese Direct Investment and Dutch National Security", The Clingendael Institute, 2018 **9** European Union, EU-China – A Strategic Outlook, 12 March 2019, p. 1 **10** B. Andreosso-O'Callaghan & F. Nicolas, "Complementarity and rivalry in EU - China economic relations in the twenty-first century", European Foreign Affairs Review, Vol 12, no. 1, 2007, pp. 13-38. M. Mattlin, "Chinese strategic state-owned enterprises and ownership control", BICCS Asia Paper, Vol 4, no. 6, 2009, pp. 1-28. A. Michalski & Z. Pan, "Role Dynamics in a Structured Relationship: The EU-China Strategic Partnership", JCMS: Journal Of Common Market Studies, Vol 55, no. 3, 2016, pp. 611-627 **11** Andreosso-O'Callaghan & Nicolas, op. cit., pp. 13-38. Mattlin, op. cit., pp. 1-28 **12** A. Pepermans, "The Huawei case and what it reveals about Europe's trade policy", European Foreign Affairs Review, Vol 21, no. 4, 2016, pp 539-558 **13** Scott, op. cit., pp. 217-233. J. Men, "The EU and China: mismatched partners?", Journal Of Contemporary China, Vol 21, no. 74, 2012, pp. 333-349 **14** S. Meunier, "Beware of Chinese bearing gifts: Why China's Direct Investment Poses Political Challenges in Europe and the United States", in China's three-prong investments strategy: bilateral, regional, and global tracks, C. Julien (ed.), Oxford University Press, 2018. J. Knoerich & T. Miedtank, "The Idiosyncratic Nature of Chinese Foreign Direct Investment in Europe", cesifo FORUM, Vol 19, no. 4, 2018, pp. 3-8 **15** A. Minin & J. Zhang, "An Exploratory Study on International R&D Strategies of Chinese Companies in Europe", Review of Policy Research, Vol 7, no. 4, 2010, pp. 433-455 **16** Knoerich & Miedtank, op. cit., pp. 3-8 **17** J. C. Defraigne, "Chinese outward direct investments in Europe and the control of the global value chain", Asia Europe Journal, Vol 15, no. 2, 2017, pp. 213-228. W. Rabe & O. Gippner, "Perceptions of China's outward foreign direct investment in European critical infrastructure and strategic industries", International Politics, Vol 54, no. 4, 2017, pp. 468-486 **18** Ministry of the Economy and Energy of Germany & Ministry of the Economy and Finance of France, "A Franco-German Manifesto for a European industrial policy fit for the 21st Century", 19 February 2019. **19** "France, Germany aim for euro zone reform roadmap by June", Reuters, 16 March 2018. Ministry of the Economy and Energy of Germany & Ministry of the Economy and Finance of France, op. cit. **20** China's National Intelligence Law (2017) Art. 14 "The state intelligence work organization shall carry out intelligence work according to law, and may require relevant organs, organizations and citizens to provide necessary support, assistance and cooperation." http://www.mod.gov.cn/regulatory/2017-06/28/content_4783851.htm **21** NIS Cooperation Group, "EU-wide coordinated risk assessment of 5G networks security", Report, 9 October 2019

Francesca GHIRETTI

BIO

Francesca GHIRETTI is a researcher in the field of Asia studies at Istituto Affari Internazionali (IAI), where she mainly works on projects regarding Chinese foreign policy, Italy-China and Europe-China relationship. She is a PhD candidate at King's College London, looking at the securitisation of Chinese FDI in the EU. After obtaining her Laurea Triennale in Asian languages, markets and cultures (curriculum China) from the University of Bologna, she graduated from the MSc in International Relations and Diplomacy at Leiden University and the Clingendael Institute. She interned at the European Parliament and worked for Jaap de Hoop Scheffer, former Secretary General of NATO.

College of Europe Collège d'Europe
DEPARTMENT OF EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES
Baillet Latour Chair of European Union-China Relations

College of Europe Collège d'Europe
EU-CHINA Research Centre
EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES
BAILLET LATOUR FUND

THE CHINESE PERSPECTIVE ON CYBER COOPERATION/CHALLENGES IN EU-CHINA RELATIONS

SILVIA MENEGAZZI

Introduction

In 2012, the EU and China reached the Joint Press Communiqué at the 14th EU-China Summit to strengthen the important progress achieved in the development of EU-China relations in all the fields, stating that their comprehensive partnership grew "both in width and in depth".[1] Given the importance recognized by both sides of deepening understanding and trust on cyber issues, the EU and China agreed to set up important mechanisms and diplomatic dialogue.

That said, cyber issues are often treated as a policy area of secondary importance in EU-China relations, given the priority of economic and political issues at stake, even though cyber cooperation has become an important priority for both actors' external relations. At the international level, China and the EU present themselves as active participants on cyber-security, and cooperation in the cyber area includes important platforms such as the EU-China Cyber Task Force (track 1) and the Sino-European Cyber Dialogue (track 1.5) meetings.[2] Nevertheless, Beijing and Brussels maintain different views related to cyberspace, particularly vis-à-vis the rules and principles of international law in the cyberspace and multilateral international cooperation. In the Joint Statement of the 20th EU-China Summit in 2018 both sides agreed to increase mutual trust and understanding, with the intent to enhance policy exchanges and cooperation in the cyber area and jointly promoting further development and implementation of the norms, rules and principles for responsible State behavior in cyberspace as articulated in the 2010, 2013 and 2015 reports of the UN Groups of Governmental Experts.[3] EU officials recognize that China's strategy for cyberspace and cyber governance might differ with EU's priorities and interests. Cyber security has become a top issue in the policy agenda of both China and the EU, but major divergences persist, i.e., who should govern the cyberspace, the meaning and relevance of sovereignty in the cyberspace domain, etc. Such trends also result as a consequence of China's growing relevance in international affairs – more and more European countries experienced divergences over controversial issues with regards to decisions to ban Huawei's 5G equipment in Europe.[4] In this light, the purpose of this paper is to discuss the Chinese perspective on cyber security and its governance, particularly with a focus on cyber cooperation/challenges in EU-China relations. In doing so, the following section analyses cyber governance and security recently in China. Then, it discusses the Chinese perspectives about the Global Cyber Governance (GCG) domain. Third, it highlights the challenges on cyber cooperation in EU-China relations. Then, a conclusion will follow.

China's power in cyberspace

The reconfiguration of cyber governance in China reflects two main controversial tendencies that developed in parallel in the last decade. On the one hand, attention toward the 'great Internet' is the result of a process through which China developed into a strong Internet power with more than 700 million Internet users at the end of 2015. On the other, China's growing exposure to the Internet domain challenged its power and sovereignty vis-à-vis effective management control over its citizens. The acceleration of online information is often perceived as a direct threat by the government in China. For instance, Hong Kong's Um-

brella Revolution in 2014 led to a shutdown of Internet in major Chinese cities. The role of social media in particular, appeared under attack when strict censorship was applied to major websites such as Weibo or Twitter.[5] A few years earlier, in 2009, just in the aftermath of the riots guided by the local Turkic-speaking Uighur minority, the Chinese government shut off mobile services and the Internet of residents in Xinjiang for almost six months.[6]

2017 represented the real benchmark of a new era for China's cyberspace, when China's Cybersecurity law was published (June 1st 2017).[7] Initially reformed in 2016 by a preliminary draft offered by the National People's Congress, the law has been classified as the latest effort by the current administration to acquire further control over online content and Chinese people surfing on the Internet. In fact, prior to the new law, there were only a 'bunch' of regulations dealing with Internet security and cyber threats, which were drafted by different departments on different issues: the Regulations on Security Protection of Computer Information Systems, Administrative Measures for Internet Information Services redacted by the State Council; Administrative Measures for Prevention and Treatment of Computer Viruses redacted by the Ministry of Public Security; Administrative Measures for Hierarchical Protection redacted by the Ministry of Public Security together with other ministries; and the Law on Guarding States Secrets redacted by the NPC Standing Committee.[8] In this sense, the process of law implementation proceeded in parallel with efforts to establish new key actors in charge of cybersecurity issues in China. Yet, the issue of Internet governance is also the result of transforming China into a world-class 'information society'. Specifically, it became clear to leaders in office the necessity to reinforce advanced technologies and information processes supported by a strong communication infrastructure in all the sectors of Chinese economy and society. This process started in the Jiang Zemin's era and became a key priority with the Xi Jinping administration.[9] To this extent we could see the greatest consequence posed by Internet and communication infrastructure developments in China: political leaders understood the numerous benefits and opportunities derived from information exchange while recognizing the security challenges associated with China's opening up to the cyberspace domain.

A sudden change occurred with the Xi Jinping administration at the end of 2012. Since then, the concept of 'internet sovereignty' began to be a predominant argument among political elites in Beijing and Chinese academics. Nevertheless, discord still persists within China's domestic academic discourse.[10] More specifically, disagreement relates on the one hand, to the different understanding as well as the evolution of the two key terms in the discourse, i.e., 'information sovereignty' and 'internet sovereignty'; on the other hand, it is the origin of the term 'internet sovereignty' itself. Whereas the former issue highlights a 'terminological' policy shift in the field of information and communication technologies – with the subsequent broadening of the Chinese understanding about the notion of sovereignty in the digital domain – the latter demonstrates that the issue of internet sovereignty in China has also, broader consequences, such as the necessity to pay attention to the international dimension vis-à-vis cyber security, Overall, it is extremely unlikely to distinguish sharply a domestic and an international dimension when discussing about the concept of 'internet sovereignty' as China's normative position is consistently confronted with Western power's position.[11]

Cyber norms and Chinese perspectives in the Global Cyber Governance domain

China's role into the Global Cyber Governance (GCG) domain is linked to the notion of 'Internet Sovereignty' (wangluo zhuquan). Global Cyber Governance includes the set of norms, actors and institutions along which rules are generated to manage global concerns on cyber security. Despite the concept has being brought to wider international public attention by Xi Jinping in 2012, it is the concept of cyber-power (wangluo qiangguo), which deserves indeed even further attention. To what extent Chinese leaders intend to frame and portray the political narrative of China's ascent role as a cyber power in world affairs? Some authors believe the notion still to be linked with Chinese domestic political and economic dimensions. According to Creemers for instance, China's ideas about its role as 'Internet super-power' are first and foremost directed towards achieving effective control over all ICT processes within its own territory. More clearly three priorities guide Chinese behaviour, and these are: indigenization – reducing China's reliance on foreign suppliers for its 'core technologies'; socio-economic informatization – using ICT to promote Western style welfare and services; and other corollaries attached to the development of the ICT sector, i.e., surveillance and national security.[12]

The question about China's position vis-à-vis GCG brings us to discuss once again China's role at the international level and its willingness to contribute directly to cyber matters in global governance. First, it is the 'China National Cyberspace Security Strategy' released in December 2016 which highlights the current opportunities and challenges

in the cyberspace faced by Chinese leaders today. More specifically, these are: 1) a delicate balance between technological change and innovation and international cyber threats; 2) great powers competition in the field of GCG; 3) the militarization of the cyberspace; 4) the role of the international community to jointly contribute to common rules in the field of cyberspace governance.[13] The balance between technological change and international cyber threat explains China's ambivalent position vis-à-vis cyber-security issues: on the one hand it is the need to strengthen the ICT sector and the development of informatization in China but on the other, it seems evident how China envisions the need to further contribute to the development of international norms in the field of cyber governance.

Second, the release of the 'Report on China Internet Development' in 2017 brought broad attention to China's expanding role in the field of cyber governance, and it is well known today how China's priorities in the cyberspace and digital domains have become a hot topic in international politics. Just think of how the US-China trade war is at the heart of the battle for tech supremacy, which also includes artificial intelligence (AI), robotics, autonomous vehicles, 5G technology, etc. As it is now known, many believe that what is really behind a new "Cold War 2.0" between China and the United States is not a simple race to conquest world's supremacy about trade but cyber activity and its global predominance.[14] Considering the report as a point of reference, it is interesting to highlight also the political narrative emerging from it, which often stresses the relevance of cyber security to the Xi Jinping administration. It was in fact in 2014 that the Central Cyberspace Affairs Commission was created - an institutional body directly under the strict control of the Chinese Communist Party Central Committee in charge of all Internet-related issues and of which Xi Jinping is the leader in charge. Unsurprisingly, the report refers to Xi Jinping's "four principles for promoting the Global Internet Governance system reform" and the "five proposals for constructing a community of shared future in the cyberspace".[15] The report then recalls the International Strategy of Cooperation on Cyberspace – the white paper jointly released by the Chinese Ministry of Foreign Affairs and the Cyberspace Administration of China on 1 March 2017. The document concerns China's cyber-strategy on multilateral frameworks and organizations. In the past few years, China intends to promote cyber security 'normative dialogue' at three different levels: a) unilateral, i.e. promoting its own understanding vis-à-vis cyber governance mostly through certain initiatives, like the World Internet Conference; b) bilateral, i.e., implementing cyber governance cooperation with the United States and the European Union; c) multilateral, i.e., through a series of initiatives and dialogues: with members of SCO and BRICS; within the ARF; through the Conference on Interaction and Confidence Building Measures in Asia (CICA); through the Forum on China-Africa Cooperation (FOCAC); through the China-Arab States Cooperation Forum; the Forum on China and the Community of Latin American

Countries; through the G20 and APEC. China's behaviour appears to be in harmony with the majority of Western developed democracies, that is, its willingness to implement GCG through effective multilateralism and with the help of all major global governance institutions involved. Yet, the way through which China engages with other countries on cyber issues rests within a narrative aimed at reinforcing China's core interests. The section titled "the Principle of Sovereignty" deserves particular attention, because it is precisely the one that distances the most Chinese ideas on cyber governance from third parties in the West. More practically:
"Countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in, condone or support cyber activities that undermine other countries' national security".[16]

From a Western-European perspective, the above statement undermines the possibility of establishing a fair balance between international laws in the cyberspace and the Chinese interpretation of the sovereignty principle. More specifically, from an EU perspective, protecting the free and open Internet was envisioned as a key priority in the EU Cybersecurity strategy already in 2013. In a briefing published by the European Parliament on EU Cyber Diplomacy, China's interference with privacy and human rights are deemed to be major constrains on EU-China cooperation in the field, within which the support for the principles of non-intervention and sovereignty clashes with EU's priorities.[17] According to Dong Qingling, discrepancies between Chinese and foreign officials over the global debate on cyber security and its norms are central to an initial conundrum, that is, how to define first and foremost cybersecurity. In his view, whereas Chinese government takes cybersecurity as technological safety and political stability, cybersecurity means technological resilience, intellectual property rights and data protection to the US.[18] Overall, it demonstrates the need to further contextualize EU-China divergence about cyber norms on a broader level, as norm contestation also stands as a common practice of global politics. In the EU's case, the normative contribution is different from that of China, given that the EU is in favour of a set of principles among which universal access to the Internet and freedom of opinion and expression represent its two essential elements.

EU-China cyber relationship: challenges ahead

There are a number of themes that both the EU and China currently prioritize which could be offered as areas to explore in future engagements. Nevertheless, European and Chinese approaches to cybersecurity are divergent.
First, whereas the EU continues efforts to enhance concrete developments concerning the norms, rules and principles of responsible state behavior in the cyberspace, China's Cybersecurity Strategy specifies the country's ambitions to guarantee the preservation of its critical information infrastructure as well as preserving cyberspace sovereignty and protect national security.

Second, China's National Cyberspace Security Strategy states that international competition is on the rise. China's views on the global cyberspace are framed within a context of great power competition in which "individual countries have strengthened their network deterrence strategies and intensified the cyberspace arms race, and world peace has been challenged by new challenges".[19] For this reason, the EU-China Cyber Task Force was launched in 2012 and the 7th EU-China Cyber Task Force was held in Beijing on January 2020. Among the major topics discussed during the meeting include the overall situation in cyberspace, international rule-making processing, 5G and digital economy.[20] The Sino-European Cyber Dialogue, too, is aimed at reducing 'misperceptions and to increase transparency of both countries' authorities and understanding on how each country approaches cybersecurity and to identify areas of potential cooperation, including the application of international law, confidence building measures and agreement on norms of responsible behaviour'.[21] However, the core of the Chinese strategy vis-à-vis cyber issues is strongly rooted in non-interference in international affairs, an approach that profoundly differs with EU's ideas and practices in the cyberspace domain. Having said this, one possible area of exchanges and good practices could be to increase the equal participation of states in dealing with international decision-making in the cyberspace arena, given the mutual importance presumed by both China and the EU in the process of cyber norms implementation. Similarly, support for the United Nations and other multilateral institutions could further strengthen EU-China cyber cooperative efforts by implementing deeper interregional EU's engagement in Asia.

Overall, the EU already perceives China as a key player to strengthen its engagement in GCG. EU cyber partnerships are in fact a priority to envision EU's role as a global actor. Yet China, will continue to push its own diplomacy and

agenda on cyber sovereignty and the EU must face this challenge by questioning to what extent it is ready to cope with China's growing posture as a major cyber power in international relations.

Conclusions

In analysing China's position and political narrative about cyber governance and security, this paper has shown the relevance of such issue in the context of EU-China relations. From a Chinese perspective, cyber cooperation with the EU is welcome as far as the principles of non-intervention and sovereignty are respected and therefore applied to the cyberspace context. However, from an EU perspective, China is part of a broader picture when it comes to the issue of cyberspace and its governance, that is, as part of a group of countries through which collaboration is needed to strengthen the EU's values and principles on virtual and digital levels.

Nevertheless, in recent times growing concerns about 5G technology and Chinese state security laws also jeopardised EU-China cyber cooperation.

There is a growing awareness in Brussels about Beijing's ascent cyber power, which is contributing to EU's concerns about the need to constantly monitor China's behaviour in the cyber sphere.[22] Whereas China recognizes the fact that the EU's support of international laws with respect to cyber governance might not match with its own, Chinese leaders are disappointed that China is perceived as a threat in international affairs by some countries. If China and the EU are willing to enhance cooperation on cyber security, the greatest challenge is about norms convergence, but perceptions and trust between the two will also matter in the foreseeable future. ©

1 Council of the European Union, Joint Press Communique of the 14th EU-China Summit, 6474/12, PRESSE50, Beijing, 14 February 2012 **2** "Sino-European Experts Working Group on the Application of International Law in the Cyberspace", Geneva Centre for Security Policy, 5 June 2019, retrieved 20 September 2019, https://www.gcsp.ch/global-insight/sino-european-expert-working-group-application-international-law-cyberspace **3** "Joint statement of the 20th EU-China Summit", EEAS Website, 17 July 2018, https://eeas.europa.eu/delegations/china_en/48424/Joint%20statement%20of%20the%2020th%20EU-China%20Summit **4** "Huawei: US and Europe divided as Germany officially rejects Washington's demands", Forbes, 14 April 2019, retrieved 23 September 2019, https://www.forbes.com/sites/zakdoffman/2019/04/14/huawei-u-s-and-europe-divided-as-germany-formally-rejects-washingtons-demands/#1ac07f133bea **5** "Social Media and the Hong Kong Protests", The New Yorker, 1 October 2014, retrieved 24 July 2017,https://www.coleurope.eu/system/tdf/uploads/page/authors_note_20180213.pdf?&file=1&type=node&id=22518&force= **6** "Xingjian, tense Chinese region, adopts strict Internet controls", The New York Times, December 2016, https://www.nytimes.com/2016/12/10/world/asia/xinjiang-china-uighur-internet-controls.html **7** For the full text of the China Cybersecurity Law see China Copyright and Media: https://chinacopyrightandmedia.wordpress.com/2016/11/02/cybersecurity-law-of-the-peoples-republic-of-china-third-reading-draft/ **8** "Overview of China's Cybersecurity Law", KPMG China, February 2017, retrieved 23 September 2018, https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf **9** G. Austin, Cyber Policy in China, Cambridge&Malden, Polity Press, 2014. **10** J. Zeng, T. Stevens and Y. Chen, "China's solution to Global Cyber Governance: unpacking the domestic discourse of Internet Sovereignty", Politics &Policy, Vol.45, n.3, 2016, pp. 432-464. **11** Ibid., Zeng, Stevens and Chen, 2016. **12** R. Creemers, "The Pivot in Chinese Cybergovernance. Integrating Internet Control in Xi jinping's China", China Perspectives, 2015/4, pp. 5-13. **13** See for instance, Kimberly Hsu, "China and International Law in the Cyberspace", US-China Economic and Security Review Commission Staff Report, 6 May 2014. See also Scott Warren Harold, Martin C. Libicki and Astrid Stuth Cevallos, Getting To Yes with China in Cyberspace, RAND Corporation, 2016. **14** "The Cold War between China and the US is already a virtual reality", The Conversation, 2019, retrieved 20 November 2019, http://theconversation.com/the-cold-war-2-0-between-china-and-the-us-is-already-a-virtual-reality-125081 **15** "Report on China Internet Development 2017", Cyberspace Administration of China, 2017, retrieved, 27 March 2019, http://www.cac.gov.cn/1122128829_15135790794381n.pdf **16** "Full Text: International Strategy of Cooperation on Cyberspace", Xinhua, 1 March 2017, retrieved 22 March 2018, http://www.xinhuanet.com/english/china/2017-03/01/c_136094371_2.htm **17** European Parliament, "Cyber Diplomacy. EU dialogue with third countries", Briefing, June 2015, pp.1-12. **18** "Confidence Building for Cyber Security between China and the United States", CIIS, 23 September 2014, retrieved 17 March 2019, http://www.ciis.org.cn/english/2014-09/23/content_7254470.htm **19** Full Text China's National Cyberspace Security Strategy", Cyberspace Administration Agency, http://www.cac.gov.cn/2016-12/27/c_1120195926.htm **20** "The 7th EU-China Task Force was held in Beijing", Chinese Ministry of Foreign Affairs, 13th January 2020, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/jkxw_665234/t1731937.shtml **21** 7th Sino-European Cyber Dialogue (SECD) takes place in Geneva, https://hcss.nl/news/7th-sino-european-cyber-dialogue-secd-takes-place-geneva **22** "EU eyes tougher scrutiny of China cyber security risks", Financial Times, 2 January 2019, https://www.ft.com/content/3d13c208-0545-11e9-99df-6183d3002ee1

Silvia MENEGAZZI

BIO

Dr Silvia MENEGAZZI is Adjunct Professor in International Relations at the Department of Political Science at LUISS Guido Carli University. She has been Visiting Research Scholar at the China Foreign Affairs University in Beijing (2014) and at the University of Warwick (2016). She holds an MSc in International Politics from the School of Oriental and African Studies (SOAS) in London and a MA in East Asian Studies from La Sapienza in Rome. She speaks Chinese fluently and has spent long periods of time in China (Nankai University, Beijing Foreign Studies University, Renmin University, East China Normal University). Her research interests include International Relations Theory, Asian Politics and society, EU foreign policy in Asia, think tanks and non-governmental actors of contemporary China. Among her recent publications, Rethinking Think Tanks in Contemporary China (Palgrave Macmillan, 2017) and New Regional Initiatives in Chinese Foreign Policy. The Incoming Pluralism of Global Governance (Palgrave Macmillan, 2018 with M. Dian).

College of Europe Collège d'Europe
DEPARTMENT OF EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES
Baillet Latour Chair of European Union-China Relations
College of Europe Collège d'Europe
EU-CHINA Research Centre
EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES
BAILLET LATOUR FUND

CONTOURS OF AN EFFECTIVE COMPETITION POLICY: PROMOTING EUROPE 'AS A' DIGITAL CHAMPION (AND 'NOT' EUROPEAN CHAMPIONS!)

KALPANA TYAGI

Introduction

The rise of China Inc. and the digitalization of even the most traditional, bricks and mortar sectors of the global economy has led many to persuasively argue that the EU competition policy is 'obsolete' and needs a re-think.[1] In this paper, I highlight the underlying factors that validate (or invalidate) these concerns and explore how these two challenges that emerged simultaneously can be managed within the existing legal framework, and wherever required, may be effectively handled with suitable policy reforms. In section two, I very briefly discuss the Commission's prohibition decision on Siemens/Alstom, and the reasons that led to a call for reform of the EU competition policy. Section three discusses how digitalization in general, and the acquisition of promising digital start-ups by firms from third countries may raise legitimate concerns of public scrutiny, and why such acquisitions merit a review. Against the backdrop of findings in section two and three, section four discusses how the distinctive nature of emerging China Inc. merits due attention for any meaningful debate on EU competition, trade and industrial policies. Section five concludes.

Siemens/Alstom prohibition (& the call for European Champions)

In February 2019, the European Commission prohibited the merger between Siemens and Alstom. The parties' principle economic rationale was to combine their 'complementary product offerings and geographic footprints' to competitively respond to emerging mobility challenges, and effectively counter the 'increasing competitive pressure from rapidly growing (Chinese/Asian) competitors'.[2] This was not only one of the very rare instances where the Commission prohibited a merger, but also one of those extremely rare cases where the European Commission and the National Competition Authorities' assessment stood in clear contrast to that of the National Governments, most notably, the French and the German governments. Siemens, Alstom and their respective national governments were principally concerned with the emerging threats of digitalization and automation in the era of Industry 4.0 and the strength of the China Railway and Rolling Stock Corporation (CRRC) as the world's leading supplier of high-speed trains.[3] The Commission, however, was unconvinced of the CRRC's strength or its possible entry in the EU 'in the foreseeable future'[4] and identified that the merger could negatively impact competition in the market for high-speed trains in Europe.[5]

The founding fathers of the European Treaties identified EU competition law as the key to achieving a European single market to facilitate the free flow of goods and services across the Union.[6] Shortly after the Commission's decision, the two governments, along with the Polish government released a joint manifesto that envisioned an industrial policy for a competitive Europe in the 21st century.[7] The emergence of two macro-economic dynamics – the China Inc. (section three) and Digitalization (section four) – has challenged[8] this well-defined and insulated (from the larger industrial policy objectives) role of competition policy that has so far fared well in tiptoeing towards a single market.

Digitalization

The emergence of the digital economy has put 'data' center-stage in the competition policy debate. Data has always been important for firms to understand and be

more responsive to the needs of their customers. However, the emergence of big data and the rise of the platform economy mean that for any firm to remain competitive, access to data is essential to compete effectively in the market. The digital economy has certain distinct features – such as network effects, learning effects and customer lock-in – that distinguish it from the traditional bricks and mortar economy. Network effects mean that the value of the network increases as a square of the number of its users. For example, if the number of users of a network increases from 2 to 10, then the value of the network increases from 4 (that is 22) to 100 (102). Considering the time and learning required to adapt to a given network or a new technology, the platforms also enjoy a learning or a lock-in effect. Consider for instance, the challenges associated with converting MS Office users into Apple Mac users or vice versa.[9] Coupled with these advantages in the Information Communications Technology (ICT) sector, the falling costs of storing data and the increasing use of algorithms mean that digital economy today is controlled by a handful of firms.[10] The EU competition policy, with suitable adaptations can effectively meet these challenges of digital economy.[11] The emergence of China Inc. and its beguiling interaction with this digitalization, as discussed in the section that follows, however, presents some novel challenges that require looking beyond EU competition law, and more towards the common commercial policy of the European Union.

China Inc.

In light of the very special nature of platform economics and digitalization, the platform economy tends to tip towards a handful of global players. In addition to this challenge, the EU legal order is increasingly confronted with another novel issue – the rise of China Inc.

In China one observes a rather 'paternalistic system' wherein the government looks at different legislative instruments as a connected whole, united by the larger industrial policy goals of the Chinese Government. This 'paternalistic system' of China Inc. functions effectively because bureaucrats and other high ranking public officials, thanks to the Confucian philosophy, are early on nurtured with virtues such as 'honesty, trust and compassion' and cultivated to be subservient to the larger policy objectives of the State.[12] To further add to the complexity, China has a very sui generis system, wherein state-run and state-sponsored enterprises compete for market shares in highly competitive markets. Mark Wu calls this China Inc.[13] This means that the State, the State Owned Enterprises (SOEs) and the private enterprises co-ordinate and operate in sync to achieve the larger goals of the State.

China's rapid rise as the world's leading economy in a remarkably short period of time has attracted both praise and criticism of scholars.[14] One of the commonly encountered criticisms is how China pursues an industrial policy-driven approach through its paternalistic and

centralized decision making process. If on the one hand, availability of low-cost goods manufactured in China has made them more accessible to the world population at large, then on the other hand, this has often been criticized and contested in international settings as the dumping of cheap Chinese goods.[15] This has not only led to the complex trade policy challenges such as contesting the dumping of cheap Chinese goods and the consequent refusal to grant a Market Economy Status (MES) to China[16] or the 'discriminatory treatment of foreign firms' investing in China,[17] it also led to the complex geo-strategic challenges of dealing with incoming (state- subsidized) foreign investment from China in the recipient countries. It is often stated that the Chinese investments overseas are not entirely driven by the market principles of a free functioning economy. These investments are rather part of a larger plan of the State, such as the 'One Belt One Road' (OBOR) initiative.[18] In fact, it was this highly debatable infrastructure financing of international Chinese projects that led Siemens and Alstom, discussed in section two above, to propose their merger in order to compete with the Chinese CRRC at a global level. This was also the reason why the two firms, as well as their respective governments argued that the competition for high and very high speed trains existed at a worldwide level, with the Chinese State-led firms giving tough competition to private firms from across the globe.[19] This conflicting position of the parties and the Commission well highlights the conflict that may arise between trade and competition policy.[20]

THE CHINESE INVESTMENTS OVERSEAS ARE NOT ENTIRELY DRIVEN BY THE MARKET PRINCIPLES OF A FREE FUNCTIONING ECONOMY.

As the foregoing discussion illustrates, the approach of China Inc., stands in contradistinction to the more well-defined approach of the EU.

When Digitalization and China (Inc.) meet….

The peculiarities of the platform economy, and the data-driven nature of the digital economy in particular has led to the entrenched positions of dominance of the digital platforms. In addition to these inherent advantages, China Inc. offers its enterprises – whether state-owned or private – a supplementary strategic advantage. A notable success of this coordinated approach by China Inc. is the success of its digital firms such as WeChat, offered by the Chinese conglomerate Tencent. Tencent is a Chinese digital conglomerate, active in a range of services – ranging from e-commerce to social networking sites. All these services revolve around its networking site QQ and WeChat and have benefitted significantly from the 'protected market conditions' in China.[21] Whereas Tencent's benefits have largely emerged from protected domestic markets – which from the perspective of foreign investors is a 'market access' issue, and therefore, more effectively dealt with by the WTO and trade laws;[22] Chinese firms – both Chinese SOEs and private firms - have benefited significantly from the State funding for the acquisition of foreign firms.[23] This means that that foreign direct investment (FDI) in many circumstances may not be market-driven. Even though the FDI plays a key role in promoting development and job creation in the host state, it is absolutely crucial that the FDI must not adversely impact the latter's security and internal order.

Conclusion

With an average annual growth rate of 6.8 percent over the past several decades, China today is the world's largest economy in terms of purchasing power parity.[24] Home to the world's second largest number of Fortune 500 companies, largest number of banks in the world's top 100 banks, leading tech companies such as Alibaba and Tencent, China Inc. today is 'deeply integrated' into the world economy.[25] Considering its economic and demographic significance as the world's most populated economy, it is extremely vital to ensure that China Inc. is successfully integrated in the fabric called global trade. This is particularly important as how China Inc. functions today impacts not only China, but the world economy at large.

Whereas the reform of the EU merger control may be in good spirit to confront the challenges thrown in by digitization, the CCP is a more suitable instrument to deal with the FDI-related issues.[26] With the implementation of the Lisbon Treaty, the European Parliament plays an increasingly important role and uses the ordinary legislative process (OLP) for deciding most trade policy related issues.[27] Competition rules on the other hand are managed by the European Commission's Director-General for Competition, with the Council of the EU and the European Parliament's minimalistic intervention in the area.[28] Any abrupt change to accommodate certain national interests will only disrupt this well-defined legal order of the Union.

Furthermore, as our discussion illustrates, it is true that foreign investment may oftentimes not be market driven. This challenge notwithstanding, policy makers must never lose sight of the underlying principle of EU competition policy, that is to establish 'workable and effective competition'[29] in the internal market. If regulating foreign investment is important to ensure national security, then capital liquidity through foreign investment is key to safeguard digital innovation and entrepreneurship, two key challenges confronting the digital single market.

In this article, on account of the word limit, I restrain my discussion to issues that can and must be addressed by EU competition policy to ensure workable competition in the internal market. A comprehensive discussion on FDI and national security calls for a critical analysis of the dynamic interplay between competition policy and foreign investment screening. [30] ©

1 Bundesministerium für Wirtschaft und Energie and Ministère de l'Économie et des Finances, 'A Franco-German Manifesto for a European Industrial Policy fit for the 21st Century' N°1043 (Paris 13 February 2019) <https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/02/1043_-_a_franco-german_manifesto_for_a_european_industrial_policy_fit_for_the_21st_century.pdf> accessed 4 December 2019. **2** Siemens/Alstom (Case No COMP/M.8677) [2019] OJ/C300/06, para 9. A detailed assessment of the merger is beyond the scope of the present article. For a detailed critical analysis, see Kalpana Tyagi, 'Commission's decision in Siemens/Alstom: 'An Economic Error & a Political Mistake' or Prohibition to Promote Competition on the Merits?' (Forthcoming, copy available with the author on request) **3** Ibid. **4** Siemens/Alstom, paras 497, 1048-1098, 1166-67. **5** Siemens/Alstom, paras 563, 859, 897, 908, 1094-1102, 1284. **6** Robert Schütze, European Union Law (Cambridge University Press (2nd ed.) 2018) 711. **7** Bundesministerium für Wirtschaft und Energie, Ministère de l'Économie et des Finances and Ministerstwo Przedsiębiorczości I Technologii, 'Modernising EU Competition Policy' (04 July 2019) <https://www.bmwi.de/Redaktion/DE/Downloads/M-O/modernising-eu-competition-policy.html> accessed 4 December 2019. **8** Supra note 1. **9** Kalpana Tyagi, Promoting Competition in Innovation through Merger Control in the ICT Sector: A Comparative and Interdisciplinary Study (Springer 2019) <https://www.springer.com/gp/book/9783662587836>. For a detailed discussion on the distinct features of the sector, see Chapter 3: Salient Features of the ICT sector **9** Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the Digital Era: Final Report' (2019) European Commission <e> accessed 4 December 2019. **11** Ibid. **12** Mel Marquis and Jingyuan Ma, 'Confucian Bureaucracy and the Administrative Enforcement of Competition Law in East Asia' (2018) Vol. XLIII North Carolina Journal of International Law, 15ff. **13** Mark Wu, 'The "China, Inc." Challenge to Global Trade Governance' (2016) 57 Harvard International Law Journal, 1001ff. **14** See Kalpana Tyagi, 'China's pursuit of Industrial Policy Objectives: Does the WTO (really) have an answer?' 54(4) Journal of World Trade 2020 (forthcoming). See also the references therein. **15** Ibid. **16** For an excellent discussion on the response of the US trade law to the emergence of China through different instruments such as antidumping, countervailing duties, safeguards and managed trade, see Wentong Zheng, 'Trade Law's Responses to the Rise of China', 34(2) Berkeley Journal of International Law, pp. 110-158. **17** For a discussion of discriminatory treatment of foreign firms in China, and the pros and cons of various policy responses – such as the World Trade Organization (WTO), the Chinese continued Non-Market Economy status (NME) or unilateral tariffs, as imposed by the US lately, see Supra Note 12. **18** Vittorio D'Aleo, Giacomo Morabito, Walter Vesperi, Roberto Musotto, David Di Fatta and Salvatore Lo Bue, 'Abenomics and Active Pacifism: How Abe's Age Influenced the International Business' in Bryan Christiansen and Fatmanur Kasarci (eds), Corporate Espionage, Geopolitics, and Diplomacy Issues in International Business (IGI-Global, 2017) 21-22. **19** Leo Klimm und Alexander Mühlauer, 'Frankreich und Deutschland wollen ein neues Kartellrecht' (6 Februar 2019, Brüssel) Süddeutsche Zeitung <https://www.sueddeutsche.de/wirtschaft/frankreich-deutschland-eu-kartellrecht-1.4318855> accessed 4 December 2019. **20** Jordi Gual, 'The Three Common Policies: An Economic Analysis' in Pierre Buigues, Alexis Jacquemin and André Sapir (eds.), European Policies on Competition, Trade and Industry (Edward Elgar 1995) 15-21. **21** Yue Wang, 'Could the Worst be Over for China's Tencent?' (28 March 2019, Online) Forbes <https://www.forbes.com/sites/ywang/2019/03/28/could-the-worst-be-over-for-chinas-tencent/#319afa8a6500> accessed 4 December 2019; Arjun Kherpal, 'Tencent's Profit Beats Market as Analysts Predict Stock will climb back above $500 billion in Value' (13 August 2019, Online) CNBC Markets <https://www.cnbc.com/2019/08/14/tencent-earnings-preview-gaming-wechat-pay-to-drive-profits.html> accessed 4 December 2019. **22** See Supra Note 12. **23** Ibid. **24** International Monetary Fund, 'World Economic Outlook Database' (October 2019) <http://statisticstimes.com/economy/countries-by-gdp-ppp.php> accessed 22 February 2020. **25** See Supra Note 12. **26** For a critical discussion, see Clemens Fuest, Achim Wambach, and others in Zäsur in der europäischen Wettbewerbs- und Industriepolitik: Freie Fahrt für Europäische Champions? <https://www.ifo.de/DocDL/sd-2019-08-fuest-etal-europaeische-industriepolitik-2019-04-25.pdf> accessed 20 January 2020. **27** Holly Jarman, 'Trade Policy' in Nikolaos Zahariadis and Laurie Buonanno (eds) The Routledge Handbook of European Public Policy (Routledge, 2018) pp. 206-207. **28** Angela Wigger and Hubert Buch-Hansen, 'EU Competition Rulkes and The European Integration Project' in Nikolaos Zahariadis and Laurie Buonanno (eds) The Routledge Handbook of European Public Policy (Routledge, 2018) p. 75. **29** See for example Hans von der Groeben in CEC, Ninth General Report on the Activities of the Community (1966), p.59. **30** Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 Establishing a Framework for the Screening of Foreign Direct Investment into the Union.

Kalpana TYAGI

BIO

Dr Kalpana TYAGI (PhD, summa cum laude) comes with over 9+ years' research and teaching experience across Europe, Asia and the USA. A qualified lawyer, Dr. Tyagi has also practiced as a legal consultant across China, Singapore and Brussels. Dr. Tyagi has received international fellowships in both law and business strategy across Asia (International Education without Borders Fellowship, Dubai) for her best research paper on M&As in India and China, USA (Lee Iacocca Fellow) and the EU (Erasmus Mundus and Max Planck Fellow in Competition and Innovation, München). Dr. Tyagi pursued her LLM, with majors in International and minors in Chinese business laws across Singapore and Shanghai. She has also worked in London and then as a research policy analyst at International Telecommunications Union, Geneva. Currently working at the University of Århus, Denmark, Dr. Tyagi works on, and writes about competition and trade policy in the age of digitalization.

College of Europe Collège d'Europe
DEPARTMENT OF EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES
Baillet Latour Chair of European Union-China Relations
College of Europe Collège d'Europe
EU-CHINA Research Centre
EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES
BAILLET LATOUR FUND

DATA PROTECTION IN EU-CHINA RELATIONS - A CASE OF EVOLVING EU ACTORNESS?

ANNIKA LINCK

Introduction

The EU is considered a global frontrunner when it comes to data protection.[1] The General Data Protection Regulation (GDPR) entered into force in May 2018 and similar rules have been adopted, for instance, in Brazil, California or India.[2] In China, the 'National standard (in pinyin 'guobiao' for national standard) on Information Technology – Personal Information Security Specification'[3] (will be rereferred to as the 'Chinese national standard' below) entered into effect in May 2018.[4] According to analysis by legal experts, this standard is similar in many aspects to the EU's General Data Protection Regulation (GDPR) and was even "written with GDPR in mind".[5] In the People's Republic of China (PRC), standards are divided into mandatory and non-mandatory ones. The national standard on information security falls in the second category. Despite not being mandatory, it is likely to serve as a technical reference to public authorities to establish whether companies are following Chinese data protection rules.[6] The Chinese national standard, adopted by the Standardization Administration of China (SAC), is expected to help enforce existing data protection rules in Chinese Criminal Law and in the Chinese Cybersecurity Law of 2017.[7] In addition to this national standard on data protection, the Chinese government has developed a comprehensive legal framework of internet regulation.[8] Data protection is mentioned in many different pieces of Chinese legislation and rules, including the Cybersecurity Law of 2017.[9]

Why does China regulate data protection? Data protection is not considered as a fundamental right in the PRC's constitution. While the Chinese constitution mentions the right to privacy, there seems to be a conceptional gap between the understanding of privacy between the EU and China, not to mention the differences in the legal systems.[10] With this paper, the author intends to explore China's potential motives for rule-making in the area of data protection. This paper focuses on external motives by examining the EU as one potential factor (as opposed to internal ones) that may have contributed to the development of a more comprehensive data protection regime in China. For this purpose, this paper will apply the concept of 'EU actorness' to the case of data protection in EU-China relations. Following Bretherton & Vogler (2006) and building on Sjörstedt (1977), this paper will assess the EU's external actorness along its three components: opportunity, presence and capability.

To what extent has the EU developed capacity to influence others in data protection?

The question of how to conceptualize and assess external influence has been a long debated one, especially for the EU due to its sui generis nature. One concept often applied to examine the ability of the EU to influence other actors is 'EU actorness'. Sjöstedt describes EU actorness as the "ability to function actively and deliberately in relation to other actors in the international system".[11] Other determining factors of EU actorness are autonomy and other state-like characteristics.[12] After first definition by Sjöstedt in 1977, the conditions for actorness have been refined and the concept developed further.[13] For the purpose of this paper, we will follow Bretherton & Vogler as well as Damro, Gstöhl & Schunz.[14] Bretherton & Vogler define actorness along three terms: opportunity, presence and capability. Opportunity represents the external environment in terms of the 'structural context of action' and thus the general external environment in terms of ideas, international norms,

interests and behavior.[15] Presence on the other hand refers to the capacity "to exert influence beyond its borders" by the mere fact of existence.[16] Presence can be evaluated e.g. by assessing whether the EU has legal competence in a certain policy area and if it has developed internal policy on this specific topic.[17] Lastly, capability looks at whether there are specific instruments or measures in place that would allow the EU to act, thus, "the availability of and capacity to utilise policy instruments" and the "ability to formulate priorities and develop policies".[18] While the concept of EU actorness is generic, it can be applied to different policy areas. There is an emerging field of research applying EU actorness to the cyber space.[19] Following Gstöhl, Damro & Schunz (2018), this paper will conduct a short analysis of the different dimensions of EU actorness (opportunity, presence, capability) in the policy area of data protection, evaluating them according to the "heuristic device" scheme 'strong', 'moderate', 'weak' and then conclude with a summary statement on the overall degree of actorness ('high', 'medium', 'low'),[20] Has the EU developed presence in the cyber policy, especially data protection, and has it influenced the adoption of data protection rules via established EU-China dialogue formats (capability)? Has the external environment (opportunity) been favourable? To what extent may the case of the Chinese national data protection standard be a case of evolving EU actorness and a sign of the EU's emerging cyber power?[21]

Opportunity

Observers have described the Snowden revelations in 2013 as a major turning point in the discussions around privacy and data protection. For the first time, evidence was brought forward, which showed a structure of universal surveillance of online interactions. It was also at the backdrop of these revelations that the GDPR, which had been stalling for some time in the EU legislative process, was finally adopted in 2016 and entered into force two years later.[22] The GDPR was followed closely by governments around the globe, and inspired legislation in e.g. California, Brazil, and others[23]. At the same time, there had already been, what could be considered a general consensus or at least a basis for universal understanding of this topic: the right to privacy or private life is enshrined in the Universal Declaration of Human Rights (article 12).[24] While data protection is a separate fundamental right enshrined in the EU Charter of Fundamental Rights (article 8), it is derived from the right to privacy.[25] Therefore, I consider the dimension 'opportunity' of actorness to be strong.

Presence

According to Christou (2014), the EU Cybersecurity Strategy of 2013 "represented the first ever attempt to set out clear priorities for the protection of cyberspace".[26] Prior to this, cyber policy was dispersed across many Regulations and Directives, and key dimensions (in particular cyber defence) were missing.[27] The EU's cybersecurity policy is driven by security, economic (internal market), legal considerations and fundamental rights concerns.[28] In addition, the bureaucratic set-up divides the topic in different sub-areas: the Directorate-General for Justice and Consumers (DG Justice) deals with cybercrime and attacks, while the Directorate-General for Communications Networks, Content and Technology (DG CNECT) deals with network and information security, among others. Cyber defense on the other hand falls under Common Security and Defense Policy (CSDP) and is taken up by the European External Action Service.[29] Christou sees in this complexity "[…] the potential difficulty for ensuring that the EU constructs a coherent and coordinated internal policy that can also be projected outwards in global deliberations on norms and principles for cyberspace behaviour.[30]"

Data protection and fundamental rights have been part of the EU's Cybersecurity Strategy of 2013, which foresees that cyberspace issues should be "mainstreamed" into EU external relations and Common Foreign and Security Policy: "The EU will place a renewed emphasis on dialogue with third countries, with a special focus on like-minded partners that share EU values. It will promote achieving a high level of data protection, including for transfer to a third country of personal data".[31] Thus, even despite the complexity in the general area of cyber policy, there seems to be a certain degree of coherence and the attempt to mainstream data protection into external relations, which may allow for this policy to be projected outwards. Therefore, presence can be considered as 'moderate'.

Capability

The concept of capability refers to how the EU can influence other international players. For instance, the policy instruments at the EU's disposal can be a good indicator to measure capability. Thus, beyond the question of whether the EU possesses the conditions to become a global actor, it is also about finding out how the EU may have had an effect. In order to examine how the EU may have influenced China's data protection regime, this paper looks at the general framework of EU-China bilateral cooperation and relevant exchanges in cyber and ICT, which have likely been the fora of engagement for official exchanges on data protection between the EU and China.

The EU-China 2020 Strategic Agenda for Cooperation (2013) aims at furthering "a peaceful, secure, resilient and open cyber space" and "promoting mutual trust and

cooperation through such platforms as the EU-China Cyber Taskforce".[32] Among the "key initiatives' it mentions the aim to "reinforce the EU-China Dialogue on Information Technology, Telecommunication and Informatisation, conduct exchanges and dialogues on related strategies, policies and regulations.[33]" Thus, there are two main official dialogues between the EU and China in digital: the EU-China Cyber Task Force (led by the EEAS) and the EU-China ICT Dialogue (led by DG CNECT). The EEAS has played a leading role in the EU-China Cyber Taskforce as internal coordinator of the EU's external positions in bilateral and multilateral fora, and in some cases as the EU representative in issues of cyber diplomacy.[34] According to Renard (2018), one of the key focuses of the EU-China Cyber Task Force, as well as of the track 1.5 Sino-European cyber dialogue is to build trust via confidence-building measures.[35] However, data protection is not in the scope of the EU-Cyber Taskforce and the Taskforce can therefore not be considered as an instrument that may have influenced Chinese internal policy-making in this area.[36] In the past, the EU supported China in the development of data protection laws via technical cooperation/funding, i.e. via the Information Society Project.[37] Further, the 2016 Communication, 'Elements for a new strategy on China', states that the EU should "promote stronger privacy and data protection rights in China and insist that EU data protection rules be respected in all personal data exchanges with China".[38] It equally mentions that the EU should promote the "primacy of international standards" also in data protection.[39]

Lastly, it is important to mention that trade considerations and free flow of data rules are likely to play an important role when it comes to the EU's capability to influence other actors in data protection rules. The EU's data protection regime foresees that the EU needs to take an 'adequacy decision' for data to flow freely.[40] This has recently been attributed to Japan and there are a couple of other countries for which such decisions have been taken. When it comes to China, the process has not been officially launched, and it remains unclear if it will be opened in the near future.[41] Nonetheless, the access to the EU market and free flow of data are likely to be a major levy to engage with other

Figure 1: Summary of analysis of EU actorness

Opportunity	Presence	Capability
Snowden revelations in 2013 brought the topic to the attention of people worldwide (see analysis above).	Christou sees in this complexity "[…] the potential difficulty for ensuring that the EU constructs a coherent and coordinated internal policy that can also be projected outwards in global deliberations on norms and principles for cyberspace behaviour.[42]"	EU-China Agenda for Strategic Cooperation 2020 mentions the EU-China ICT Dialogue (DG CNECT) and the EU-China Cyber Taskforce (EEAS).[43] Thus, there is a formal structure in place to engage in dialogue.
Privacy as a fundamental right is enshrined in the Declaration on Human Rights.[44]	The EU's cyber security policy is driven by different considerations: security, economic (internal market), legal and lastly normative considerations that derive from fundamental rights concerns.[45]	Technical cooperation, e.g. EU-China Information Society Project with aim to help China develop data protection legislation.[46]
GDPR has been closely followed by governments around the globe and inspired legislation in e.g. California, Brazil etc.[47]	Nonetheless, data protection is mainstreamed into external policy. Thus, 'presence' in data protection may be more developed than cyber policy in general as there are strong rules with the GDPR (see analysis above).	'Adequacy decisions' of EU in trade agreements for free flow of data could act as an incentive for China to develop data protection regulation. Without an 'adequacy decision', free flow of data is limited.[48]
Strong	**Moderate**	**Moderate**

Following Damro, Gstöhl & Schunz 2018, p. 16.

countries on data protection legislation and rules. Overall, 'capability' can therefore be considered to be 'moderate'.

Conclusion

Applying the concept of EU actorness to the case of data protection policy in EU-China relations allowed to shed light on the potential of the EU to have influenced China in this policy area. There is some evidence that the EU has developed the ability to act and influence other actors in the area of cyber policy, especially data protection. The analysis of EU actorness in terms of opportunity (strong), presence (moderate) and capability (moderate) results in a medium to high overall level of actorness. At the same time, this conclusion needs to be read bearing in mind the limitations of the concept of 'actorness'. This paper has not yet gone into gathering empirical evidence of the actual links between the general capability and the outcome of EU engagement. A policy analysis of official Chinese documents or interviews with involved Chinese officials would need to be conducted to examine whether the adoption of certain policy elements has been the result of EU engagement – at this stage, such a conclusion is not possible as no such link has been investigated. Also, while China seems to be developing data protection regulation, these efforts may not necessarily be linked to general reforms towards strengthening on rule of law and fundamental rights. This makes it debatably whether the EU's engagement had the sought-for effect. Subsequent research will need to dive deeper into refining the analytical framework of actorness, focusing on advancing the operationalisation of the concept. Notably, there is a need to collect empiric evidence of the actual links between the EU's actorness in this field and the effect of the EU's external policy on Chinese policy making. ©

1 A. Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog", The New York Times online, 24 May 2018, available at: https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html. **2** "Data privacy law: the top global developments in 2018 and what 2019 may bring", DLA Piper, 25 February 2019, available at: https://www.lexology.com/library/detail.aspx?g=31dd432e-8c9d-4856-bacc-d7ef60b41592. **3** Official name: GB/T 35273-2017 Information Technology – Personal Information Security Specification (GB/T 35273-2017) **4** Y. Luo & Ph. Bradley-Schmieg, "China Issues New Personal Information Protection Standard", Inside Privacy online, 25 January 2018, available at: https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard/. **5** L. Louis, "China emerges as Asia's surprise leader on data protection", Financial Times online, 30 May 2018, available at: https://www.ft.com/content/e07849b6-59b3-11e8-b8b2-d6ceb45fa9d0; This view was also brought forward at a workshop at think tank ECIPE in Brussels in September 2018, which the author attended. The Chinese legal experts present at the workshop explicitly mentioned that the standard was similar to the GDPR: https://ecipe.org/events/ecipe-seminar-privacy-with-chinese-characteristics/. Other sources: Wei Sheng, "One year after GDPR, China strengthens personal data regulations, welcoming dedicated law", Technode online, 19 June 2019, available at: https://technode.com/2019/06/19/china-data-protections-law/; "China's "GDPR" Undergoes Major Upgrade – Revised Draft for Personal Information Security Specification Released", Dai Hui Lawyers, 16 February 2019, available at: http://www.dahuilawyers.com/publications/Chinas-GDPR-Undergoes-Major-Upgrade-Revised-Draft-/ **6** S. Xia, "China's Personal Information Security Specification: Get Ready for May 1", China Law Blog, 28 February 2018, available at: https://www.chinalawblog.com/2018/02/chinas-personal-information-security-specification-get-ready-for-may-1.html. **7** Y. Luo & Ph. Bradley-Schmieg, "China Issues New Personal Information Protection Standard", Inside Privacy, 25 January 2018, available at: https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard/. **8** J. Fell, "Chinese Internet Law: What the West Doesn't See", The Diplomat online, 18 October 2017, available at: https://thediplomat.com/2017/10/chinese-internet-law-what-the-west-doesnt-see/.; T. Hart "Information Governance and 'Informatisation' in China: Solutions and Plans", EU-China Information Society Project, Presentation at "Global Forum 2008, 2008. **9** Ibid. **10** In the Chinese constitution, the right to privacy is mentioned explicitly in relation to the "right to freedom and privacy of correspondence" in its article 40 (P. De Heert & V. Papakonstantinou, "The data protection regime in China", 2015, p. 17). Zhu (1997) argues that in a Chinese understanding the right to privacy is mostly associated with the right to reputation and dignity (G. Zhu, "The Right to Privacy: An Emerging Right in Chinese Law", Statute Law Review, Volume 18, Number 3, 1997, pp. 208-214.). This differs from the EU perspective on privacy and data protection. In the European Union, both privacy and data protection are fundamental rights. **11** G. Sjöstedt, "The External Role of the European Community", Saxon House, Swedish Institute of International Affairs, 1977, p. 16. **12** A. Niemann & C. Bretherthon, "Introduction: EU external policy at the crossroads", International Relations, Vol. 27. No. 3, 2013, pp. 265. **13** see e.g. J. Jupille & J.A. Caporaso, "States, Agency and Rules: the European Union in Global. Environmental Politics", Rhodes, Carolyn (ed.), The European Union in the World Community, 1998, pp. 213-229.; C. Bretherton & J., "Environmental policy. The Union as a Global Leader", in: C. Bretherton and J. Vogler, The European Union as a Global Actor, London: Routledge, 2006, pp. 89-110. **14** Ibid.; C. Damro, S. Gstöhl & S. Schunz, The European Union's Evolving External Engagement: Towards New Sectoral Diplomacies? Routledge, 2018, p. 17. **15** C. Bretherton & J. Vogler, "Conceptualizing actors and actorness", in: C. Bretherton and J. Vogler, The European Union as a Global Actor, London: Routledge, 2006, p. 24. **16** Ibid., p.24. **17** C. Damro, S. Gstöhl & S. Schunz, "The expanding scope of EU external engagement", The European Union's Evolving External Engagement: Towards New Sectoral Diplomacies?, Editors: C. Damro, S. Gstöhl & S. Schunz, Routledge, 2018, p. 16. **18** C. Bretherton & J. Vogler, "A global actor past its peak?", International Relations, Vol. 27 Nr. 3, 381, September 3, 2013, cited from: C. Damro, S. Gstöhl & S. Schunz, The European Union's Evolving External Engagement: Towards New Sectoral Diplomacies? Routledge, 2018, p. 17. **19** H. Carrapico & A. Barrinha, "European Union cyber security as an emerging research and policy field", European Politics and Society, 2018, Vol. 19, Nr. 3, pp. 299-303. **20** C. Damro, S. Gstöhl & S. Schunz, "The expanding scope of EU external engagement", The European Union's Evolving External Engagement: Towards New Sectoral Diplomacies?, Editors: C. Damro, S. Gstöhl & S. Schunz, Routledge, 2018, p. 17. **21** According to Joseph Nye Jr. 2010, cyber power is defined as 'the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power' (Nye 2010, p. 4). See: Nye, J.S. Jr. 2010. 'Cyber Power', Harvard Kennedy School, Belfer Center for Science and International Affairs, May. **22** A. Rossi, "How the Snowden Revelations Saved the EU General Data Protection Regulation", THE INTERNATIONAL SPECTATOR, 2018, VOL. 53, NO. 4, 95–111; European Commission, "Joint Statement on the final adoption of the new EU rules for personal data protection", 14 April 2016, available at: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_1403. **23** "Data privacy law: the top global developments in 2018 and what 2019 may bring", DLA Piper online, 25 February 2019, available at: https://www.lexology.com/library/detail.aspx?g=31dd432e-8c9d-4856-bacc-d7ef60b41592; José E. Pieri & A. Müssnich, "Companies Are Now Getting Ready for Brazil's New Data Protection Law", JonesDay Insights online, September 2019, available at: https://www.jonesday.com/en/insights/2019/09/brazils-new-data-protection-law; "Stringent data protection regulation has gone global", ZDNet, 24 June 2019, available at: https://www.zdnet.com/article/stringent-data-protection-regulation-has-gone-global/. **24** European Data Protection Supervisor, Data protection, available at: https://edps.europa.eu/data-protection/data-protection_en **25** Ibid. **26** G. Christou, "The EU's Approach to Cyber Security", EU-China Security Cooperation: performance and prospects, Autumn 2014. **27** Ibid. p. 5 **28** Ibid. p. 5 **29** Ibid. p. 5 **30** Ibid. p. 5 **31** European Union 2013, "Joint

Communication – Cybersecurity Strategy of the EU", Brussels, 7 February 2013, p. 15, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf. **32** G. Christou, "The EU's Approach to Cyber Security", EU-China Security Cooperation: performance and prospects, Autumn 2014, p. 2. **33** European Union 2013, "EU-China 2020 Strategic Agenda for Cooperation", p. 7. **34** G. Christou, Cyber Security in the European Union: Resilience and Adaptability in Governance Policy, New Security Challenges Series, Houndmills, Basingstoke: Palgrave Macmillan, 2016. Cited in: G. Christou, "The EU's Approach to Cybersecurity", EU-Japan Security Cooperation: Challenges and Opportunities, Spring/Summer 2017, p. 5. **35** T. Renard, "EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain", European Politics and Society, 29 January 2018. **36** Email exchange a Senior Policy Officer at the EEAS, 8 January 2020. **37** P. Pawlak & C. Sheahan, "The EU and its (cyber) partnerships", Brief Issue 9, Paris: EU Institute for Security Studies, 2014. **38** European Commission 22 June 2016, Joint Communication to the European Parliament and the Council, "Elements for a new EU strategy on China", p. 8-9. **39** Ibid. **40** European Commission 2019, "Adequacy Decisions", available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. **41** Discussion during EU-China Symposium on Data Security organised by the VUB, 29 November 2019, Brussels. **42** G. Christou, "The EU's Approach to Cyber Security", EU-China Security Cooperation: performance and prospects, Autumn 2014, p. 5. **43** European Union 2013, "EU-China 2020 Strategic Agenda for Cooperation". **44** European Data Protection Supervisor, Data protection, available at: https://edps.europa.eu/data-protection/data-protection_en. **45** Ibid. **46** P. Pawlak & C. Sheahan, "The EU and its (cyber) partnerships", Brief Issue 9, Paris: EU Institute for Security Studies, 2014 **47** Data privacy law: the top global developments in 2018 and what 2019 may bring", DLA Piper online, 25 February 2019, available at: https://www.lexology.com/library/detail.aspx?g=31dd432e-8c9d-4856-bacc-d7ef60b41592; José E. Pieri & A. Müssnich, "Companies Are Now Getting Ready for Brazil's New Data Protection Law", JonesDay Insights online, September 2019, available at: https://www.jonesday.com/en/insights/2019/09/brazils-new-data-protection-law; "Stringent data protection regulation has gone global", ZDNet, 24 June 2019, available at: https://www.zdnet.com/article/stringent-data-protection-regulation-has-gone-global/. **48** European Commission 2019, "Adequacy Decisions", available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Annika LINCK

BIO

Annika LINCK is a PhD candidate at the VUB focusing on EU-China digital legislation and policies as well as an EU Project Manager at European DIGITAL SME Alliance. As a Project Manager, she is responsible for EU-wide projects in the field of specialised skills development (IoT, Big Data and Cyber Security) and social media convergence. As a facilitator of the Working Group Cyber and Data, she follows cybersecurity and data privacy policy within DIGITAL SME, among other policy topics. In her previous positions, she been working at Huawei Technologies and as an Assistant at the College of Europe, Bruges. Annika is fluent in English, French and has an advanced intermediate level of Chinese. Her main interests revolve around how to enhance the competitiveness of the EU in the digital field, data economy, sustainable development of society and ICT skills.