Contemporary Chinese Political Economy and Strategic Relations: An International Journal Vol. 7, No. 2, August 2021, pp. 663-690

European Union's Digital Integration amidst the Diverging Interests of Its Member States: China's Involvement in EU's Digital Infrastructure

Teodora **Wiesenmayer***
Helikon Publishing, Budapest, Hungary

Abstract

The technological competition between the United States and China cannot be interpreted as a fight for technological dominance without oversimplifying the case. Digital technology is universal, and it eliminates all boundaries; therefore, its advancement strongly depends on interstate cooperation. In this context the rivals need to rely on each other; furthermore, the contribution of the consumers is indispensable because they provide the data necessary for further developments, innovations. Although the European Union strives toward a unified digital strategy, and it has elaborated the strictest regulation so far, the member states hold different views regarding their reliance on foreign technology. The development of digital technology cannot be isolated, and in this process, China seems to offer better alternatives to many European countries than the U.S. The question is whether the EU, despite the frictions among its members regarding their China policies, can diminish its dependence on the two tech superpowers, and emerge as the third greatest actor on the territory of digital technology.

Keywords: *digital technology, digital competition, the European Union's China policy, cybersecurity*

1. A Controversial Fight for Digital Supremacy

The paradigm shift entailed by the digital revolution leaves an imprint on our interpretation of foreign policy. When speaking about one of the central issues of international affairs, i.e., the technological competition between the United States and China, one cannot interpret it as a rivalry, as a fight for technological dominance, where the two adversaries are isolated entities, without oversimplifying the case. There are at least two reasons why this kind of approach would not be sufficient: the economic interdependence triggered by the globalisation and the nature of digital technology. The controversial fact regarding the latter is that although it is universal and eliminates all boundaries, its advancement strongly depends on interstate cooperation since researchers often resort to technologies developed in other countries. In this context the rivals need to rely on each other. Furthermore, the contribution of the consumers is indispensable because they provide the data necessary for further developments, innovations.

The case of the European Union also contributes to the complexity of the power relations. If it is considered as a single entity, it can be viewed as the third greatest actor on the territory – or battlefield – of digital technology. Although it strives toward a unified digital strategy, and it has elaborated the strictest regulation so far, the member states hold different views regarding their reliance on foreign technology. As it has already been pointed out, the development of digital technology cannot be isolated, and in this process, China seems to offer better alternatives to many European countries than the U.S. These alternatives include technological solutions, and less expensive products and services

offered by Chinese IT companies, e-commerce, finance, logistics and data companies (Shi-Kupfer and Ohlberg, 2019).

On the other hand, more and more countries are concerned about China's intrusion in their high-tech sector, which includes investing in companies with technologies or products that have both civilian and military applications. Besides, the Chinese government also supports cross-border R&D collaborations with Western companies or research institutes but in both cases the EU member states follow their own policies, and measure risks individually (Wang, 2019). The Trump administration considered this opposition as a fight between good and evil where the American users must be protected against "malign actors" such as the Chinese state. The Clean Network program was created to identify "untrusted apps" from China and hinder Internet traffic and data storage that involve "untrusted" Chinese carriers, cables, and clouds. But, again, the case is not so simple, since the U.S. government also practiced mass-surveillance, American tech companies exploited people's data, furthermore, the intelligence coalition named Five Eyes (including the United States, Canada, Australia, New Zealand and the United Kingdom) pressured companies to give backdoor access to all digital communications (Wang, 2021). Washington's warnings of Chinese spying look cynical after Edward Snowden's revelations on U.S. surveillance programs; therefore, it is obvious that consumers prioritize the economic considerations, and exploit the lower price of Chinese technology. Another reason why many countries prefer Chinese products and services is that so far Washington's alternative to European countries was limited to persuading them to abandon Chinese products and technologies instead of offering them efficient solutions at competent price and looking for means to lead joint research projects (Segal, 2019).

2. The Case of Huawei in the EU

The controversial nature of this fight on the digital battlefield can be best demonstrated by the case of Huawei. Although the U.S. tends to view the Chinese involvement in the EU's digital infrastructure as the intrusion of an evil power which must be eliminated, European countries consider the case on different grounds. For instance, countries like France, Germany, and the United Kingdom cannot afford a prompt ban of the company. The French cybersecurity agency, ANSSI allows operators to use Huawei's equipment until 2028. During informal conversations French authorities told operators that licenses granted for Huawei equipment will not be renewed. The French market leader, Orange, which does not use Huawei for its domestic network but relies on the company only in Spain and Poland, uses Nokia and/or Ericsson equipment for its mobile network, similarly to the other major operator, Iliad. On the other hand, Buoygues Telecom and Altice Europe will be affected strongly since they use Huawei (Reuters, 22nd July 2020). In Germany, despite the fact that the car industry might expect trade retaliations from China, moreover, it would cost companies like Deutsche Telekom, Vodafone, and Telefónica billions of euros if they decided to replace the biggest 5G supplier, tougher 5G legislation has been passed. The new IT Security Law 2.0 restricts the role of "untrustworthy" suppliers, and the government must be informed by telecoms operators if they sign contracts for critical 5G components. The United Kingdom imposed strict measures which banned buying new Huawei 5G equipment after 31 December 2020. Besides, all Huawei equipment must be removed from 5G networks by 2027. On the other hand, Huawei is still investing heavily in the UK, creating jobs and funding university research. The number of Chinese students at universities is still growing steadily, the UK-China research partnerships

have grown from 750 to 16,000 in the past 20 years, therefore the UK's complete decoupling from China seems dubious (*BBC News*, 17th May 2021).

Other EU member states also have various attitudes towards the Chinese telecommunications giant. Many of them strive for stricter measures, provided they find any evidence that will prove the U.S. warnings. The toughest actions were taken by Scandinavian and, surprisingly, Eastern European countries. Slovenia, Poland, Czechia, Romania, Estonia, Latvia, Slovakia, and Bulgaria joined the US-led coalition against Huawei in 2020. The Romanian president has recently signed a bill into law which bars China and Huawei from participating in the development of its 5G networks. On the other hand, Italy (just like France which gives the president the power to veto the acquisition of 5G parts from high-risk sources) did not ban Huawei straight away. The Italian government can veto 5G supply deals that threaten the country's national security, nevertheless, it has recently approved Vodafone's Italian unit to use Huawei for its 5G radio access network (*Euractiv*, 19th May 2021). Spain is in a difficult position, since it has strong economic ties with the U.S., whose military presence is also growing in the country, while it also has a long-standing partnership with Huawei. Despite being China's best friend in Europe – choosing a soft approach on political issues, at the same time asking China to open further its huge markets to Spanish goods and services – Spanish politicians and economists are increasingly considering China as a systemic rival due to concerns about its state capitalist model, its geopolitical ambitions, and its human rights record. Besides, the Chinese cyberattacks on Spanish public agencies and companies can further contribute to this loss of confidence (Esteban and Otero-Iglesias, 2020). Notwithstanding these concerns, Spain takes a neutral approach, delegating the assessment of risks to experts. Obligations for 5G providers and suppliers will be

specified in the forthcoming Spanish Cyber Security Act. Luxembourg, Austria, Portugal, and the Netherlands have not passed any laws yet, but telecom providers in the latter two countries announced not to resort to Huawei gear in their 5G rollout (*Euractiv*, 19th May 2021).

At this point it is worth taking a closer look at the rivalry between Huawei and its European counterparts, and the numbers behind their 5G-related patents. If the Chinese company is shut out, most probably Ericsson and Nokia will become the main suppliers in Europe. As early as 2018 Ericsson provided preliminary evidence that it was ahead of its competitors regarding the number of publicly available patent families associated with 5G declarations. (A distinction should be made between the patent applications and their approval, which can take years, therefore, the future 5G patent landscape can only be estimated.) According to the numbers released by Ericsson, in 2018 the company had nearly 700 publicly available patent families, while Huawei came out only as second with less than 500 patent families. These numbers would have been higher provided all declarations had been taken into consideration. The reason behind inflating Huawei's technological capacity is that Ericsson would be too dominant without Chinese competition, furthermore, "if Chinese companies are excluded, the only players in the 5G game are European" (Otero-Iglesias, 2019). The situation is the same in the U.S. because Huawei is among those Chinese telecommunications companies that offer "the most inexpensive, and what some European and Asian officials consider some of the best, equipment to provide the technical backbone of 5G networks" (*The New York Times*, 12th April 2019). Surprising as it may seem, there are no American suppliers for the main switching networks, which means that if Huawei is excluded, the American systems will largely be built by European firms like Nokia and Ericsson.

3. Diverging Interests of the EU Member States

The diverse attitudes of the EU member states toward China are not only reflected in their treatment of Huawei. There are many other contexts in which dealing with the EU (or Europe) as a single entity would lead only to excessive generalizations or misinterpretations. Moldicz (2019) draws our attention to the inappropriate use of the term Europe when referring only to Germany and France, adding that German and French interests should not be identified with European interests in general, either. Each EU member and non-member state assesses its relationship with China on different grounds and measures the gains and losses at various levels. In this case, the dichotomy of Western and Eastern Europe becomes irrelevant, as in most instances the economic interests determine the single states' China policy (Moldicz, 2019). On the other hand, these relations cannot be defined as static since many states keep changing their China policies according to their interests. Nevertheless, security issues should always be of priority, and each state should be able to measure the risks imposed by any kind of cooperation. Finally, it should be noted that China – despite the 17+1 initiative, where 17 states are considered as a single unit – is seemingly more aware of the sovereignty of European states than the U.S., which tends to treat Europe as a single entity (especially when it comes to trade issues), often neglecting the peculiar attributes of its states.

The EU cannot be considered as a single entity, either, regarding the issue of technology transfer, which should be considered in both directions, i.e., it can be inward and outward, functioning differently in Western and Central European contexts (*ibid.*). While the number of Western European companies complaining about being forced to hand over technology to Chinese business partners (in exchange for market access) grew considerably in 2019, many Central European countries are

interested in capital and technology transfer from China. The diverging interests of member states make it impossible to give a unanimous response to China's technological emergence.

On the whole, China's technological development impacts European trade and security interests as well. To diminish China's technological influence and the security risks, Europe must implement its own digital strategy and find those solutions that can be applicable to each member state. For this purpose, the EU must take into consideration the unique traits, the assets, and the comparative advantages of its members, and exploit this diversity. It should also keep and appreciate its talent, which is often attracted by its rivals both in the East and the West.

4. The EU's Digital Strategy and the Digital Single Market

Ursula von der Leyen presented the EU's Digital Strategy in the Communication "Shaping Europe's Digital Future". The strategic plan, which includes data, artificial intelligence, and platform regulation, intends to develop a unified Single Market for digital services to boost AI progress in Europe. It relies on the European technological success and innovation, its strong industry, and the European values. The President of the European Commission emphasised the necessity to find European solutions to global challenges, moreover, this digital transition "must protect and empower citizens, businesses and society as a whole" (von der Leyen, 2020). The strategic plan is of key importance to the EU to achieve technological sovereignty; however, it is feared that the slow legislative process will hinder the implementation of the plan.

The EU's Digital Strategy was introduced on February 19, 2020 with the aim to diminish Europe's dependence on foreign-owned technological companies, and to increase its competitiveness in a fight

for technological supremacy, where the U.S. and China are the dominant players. In her op-ed written on this occasion, Ursula von der Leyen covers all domains involved in the new strategy. First of all, she mentions the benefits of technological advancement in medical sciences, where technology contributed to a great extent to the detection and treatment of illnesses. The President expresses her wish that technology will become dominant in other fields, too: "I want it to become the norm right across our society: from farming to finance, from culture to construction, from fighting climate change to combatting terrorism". The digital transformation should be beneficial to the whole society, therefore, "Europe needs to have its own digital capacities – be it quantum computing, 5G, cybersecurity or artificial intelligence (AI)".

The core of the strategy is to help big businesses as well as small start-ups to benefit from the full potential of AI by investing in a network of local digital innovation hubs and in centres of excellence for advanced research and education. To this end, the access to big (non-personal) data pools is required, therefore, industrial players should share their data with smaller enterprises. Ursula von der Leyen argues as follows: "These types of non-personal data can underpin the design and development of new, more efficient and more sustainable products and services. And they can be reproduced at virtually no cost. Yet today, 85% of the information we produce is left unused. This needs to change". The strategy lays heavy emphasis on cybersecurity. Along with the digital transformation personal protection must be ensured, which is already provided by strict rules; however, a legislative framework and operating standards should be developed for European data spaces, which allow businesses, governments, and researchers to store their own data, as well as access data shared by others. In the European Commission's *Press Corner*, the President mentions the necessity of a unified digital single market to overcome fragmentation on the digital

ground. By creating a genuine single market for data, the strategy enables "businesses and the public sector have easy access to huge amounts of high-quality data to create and innovate". Moreover, it ensures that the data will remain secure, and data-driven products and services will respect EU rules and values.

The spectrum of the strategy is wide, it covers "everything from cybersecurity to critical infrastructures, digital education to skills, democracy to media". Besides, it is in accordance with the European Green Deal, since it promotes the climate neutrality of data centres by 2030. On the whole, the aim of the European Digital Strategy is to achieve 'tech sovereignty', which involves "the capability that Europe must have to make its own choices, based on its own values, respecting its own rules" (von der Leyen, 2020).

5. European Data Strategy and the White Paper on Artificial Intelligence

The first pillars of the European Commission's digital strategy are the Data Strategy and the White Paper on Artificial Intelligence. They are based on the defence and promotion of European values and rights, prioritizing people in the process of developing technology, and its deployment in the real economy. Creating a single market for data will ensure data availability in the economy as well as society. Data driven applications will benefit citizens and businesses in various ways, "they can improve health care, create safer and cleaner transport systems, generate new products and services, reduce the costs of public services, improve the sustainability and energy efficiency".

The European Data Strategy Factsheet provides the following examples of industrial and commercial data use:

> Jet engines filled with **thousands of sensors** collect and transmit data back to ensure **efficient operation**.
>
> Wind farms use industrial data to **reduce visual impact and optimise wind power**.
>
> Real-time traffic avoidance navigation can save up to **730 million hours**. This represents up to **€20 billion** in labour costs.
>
> Real-time notification of delayed trains can save **27 million working hours**. This amounts to **€740 million** in labour costs.
>
> Better allocation of resources to fight malaria could save up to **€5 billion in healthcare costs globally**.

The data flow, which will be provided across sectors, too, will contribute to the development of new products and services. Developing personalised medicine for patients or improved mobility for commuters are also among its numerous benefits. Besides, it will lead to productivity gains and resource efficiency. As the examples above indicate, efficient operation leads to a decrease in working hours and labour costs. According to the projections included in the Factsheet, global data volume will grow from 33 zettabytes (2018) to 175 zettabytes until 2025. The proportions of data processing will be the reverse, i.e., the centralised computing facilities will be reduced from 80% to 20% between 2018 and 2025; on the other hand, the number of smart connected objects will increase from 20% to 80% during the same period. The total investment in common European data spaces and a European federation of cloud infrastructure and services ranges between €4-6 billion. The value of the data economy of the 27 member states is expected to almost triple in these 7 years, from €301 billion to €829 billion, while the number of data professionals is expected to double, which means that their number will increase from 5.7 million in 2018 to

10.8 million in 2025. The percentage of EU population with basic digital skills would rise from 57% to 65%.

The other element of Europe's digital transformation is the White Paper on Artificial Intelligence. It provides the framework of safe AI technology development and deployment. According to the white paper entitled "Excellence and Trust in Artificial Intelligence", citizens, businesses, and governments are all among the beneficiaries of AI applications. The following benefits are mentioned in the document:

> **Citizens**
>
> Better healthcare, safer and cleaner transport and improved public services.
>
> **Businesses**
>
> Innovative products and services, for example in energy, security, healthcare; higher productivity and more efficient manufacturing.
>
> **Governments**
>
> Cheaper and more sustainable services such as transport, energy and waste management.

The paper outlines the ways in which excellence may be achieved in this field, for instance, by strengthening and connecting AI research excellence centres, or by requiring at least one digital innovation hub per Member State specialised in AI. Building trust is of equal importance in the document, which requires "high-risk AI systems to be transparent, traceable and under human control". Moreover, "[a]uthorities must be able to check AI systems, just as they check cosmetics, cars or toys", and an EU-wide debate should be launched regarding the use of remote biometric identification (e.g. facial recognition). The white paper defines high-risk AI application as its critical use in a critical sector such as

healthcare, transport, police or legal system. However, high-risk AI will be subject to strict rules and regulations. The aims of AI research and innovation can only be achieved if the EU provides the necessary funding. Although it has risen by 3% (to €1.5 billion) over the past 3 years, the aim is to attract more than €20 billion of investment per year.

6. Regulations and New Possibilities

The President of the European Commission promised to come up with legislation within the first 100 days in her office. Although the delay must be primarily due to the (at that time) unforeseen spread of the COVID-19 pandemic, some critics had already predicted the failure of accomplishing this goal on other grounds, saying that none of the documents above were legally binding, and that they were rather "an over-arching roadmap for how the EU intends to develop a single market for digital services, foster access to data and move toward hard rules for AI technology" (*Politico*, 19th February 2020). They added that although the EU planned to draft hard law on artificial intelligence in the same year, much of its details would depend on the feedback it received from industry, civil society, and national governments. At the same time, the decision was made that there would be no ban on facial recognition (partly because Brussels has limited intervention in the national governments' law enforcement, besides, the General Data Protection Regulation already includes strict rules regarding this issue). Despite the critical voices and all the difficulties posed by the pandemic, the European Commission presented its Digital Services Act package on December 15, 2020, which includes the Digital Services Act and the Digital Markets Act. These legislative initiatives have two main goals: to create a safer digital space in which the fundamental rights of all users of digital services are protected, and to establish a level playing field to

foster innovation, growth, and competitiveness, both in the European Single Market and globally. The rules of the first one concern primarily online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms.

The European Digital Strategy was endorsed by the most high-profile officials, including Margrethe Vestager, the Executive Vice-President of the European Commission (who is also referred to as the woman the Silicon Valley fears most) and Internal Market Commissioner Thierry Breton, former chairman and CEO of France Télécom, and the IT services company, Atos. When the new strategy was presented Vestager claimed that the reason why Europe could not produce a rival to Facebook or Tencent was that European businesses had never been given a full single market to expand. She added that industrial data would offer Europe a second chance to become a world leader in technology (*Politico*, 17th February 2020). The EU adopted a more pragmatic approach after it had realised that GAFA (Google, Apple, Facebook, Amazon) were too powerful to be constrained. Instead of imposing restrictions, it proposes a protectionist policy for European companies, supporting their emergence. According to this view, GAFA can be considered as the mutual enemy of European companies, and the member states should give their unanimous support in this fight. However, it is dubious whether this mutual enemy has the power to unite the supporters of a stronger, more united Europe and the countries that prefer the autonomy of nation-states (Yazdani, 2021).

As far as regulation is concerned, the EU is ahead of the two great rivals. The United States has often been criticized for the lack of any legal framework, a coherent plan to shape technology standards or ensure widespread privacy protections (Slaughter and McCormick, 2021). But China has already taken major steps: the Data Security Law (DSL), a supplement of the PRC's Cybersecurity Law, will come into

force on 1 September 2021. It applies to all data processing activities carried out within the territory of China. One of the most essential elements of the law is the one that prohibits providing any data stored in China to law enforcement authorities or judicial bodies outside the countries unless they are approved by the Chinese government. On top of that, China revealed its ambitious plan, China Standards 2035, to set global standards in emerging technologies such as 5G internet, the Internet of Things (IoT), or artificial intelligence (AI). If this plan is accomplished, China will have the opportunity to influence standards for its own benefit, moreover, it would become a recipient of licensing fees (instead of remaining one of the biggest payers). Although the Chinese put great effort in regulation, these decisions point in a different direction than the European proposals which – beside giving European companies the opportunity to emerge – focus on protecting the rights of the EU citizens.

Indeed, the EU has the most elaborate system of technological regulation. As far as cybersecurity is concerned, the role of ENISA and the Cybersecurity Act should be mentioned. The European Union Agency for Cybersecurity was founded in 2004 under the name of European Network and Information Security Agency. It works together with member states and the private sector "to deliver advice and solutions as well as improving their capabilities". The agency is also responsible for supporting the development and implementation of the European Union's policy and law on matters concerning network and information security, and for giving assistance to EU institutions, bodies, agencies, and member states. The European Cybersecurity Act (CSA), which entered into force in June 2019 and aimed to centralise and harmonise the issuing of cybersecurity certificates at the EU level, granted permanent mandate and several new tasks to ENISA. They are summarised as follows:

- Recommendations on cybersecurity and independent advice
- Activities that support policy making and implementation
- 'Hands On' work, where ENISA collaborates directly with operational teams throughout the EU
- Bringing together EU Communities and coordinating the response to large scale cross-border cybersecurity incidents
- Drawing up cybersecurity certification schemes.

The EU pays special attention to the security of its future 5G technology networks. It created a toolbox on 5G Cybersecurity, a framework of security measures "which will ensure an adequate level of cybersecurity of 5G networks across the EU, through coordinated approaches among Member States". This should be based on a common set of measures, aimed at mitigating the main cybersecurity risks of 5G networks. Besides, the toolbox also intends "to provide guidance in the selection and prioritisation of measures that should be part of national and EU risk mitigation plans". A coordinated approach needs to be applied at national and EU level, too, since network security is of strategic importance for the whole community. Among the key actions recommended for the member states and the Commission are: strengthening security requirements for mobile network operators, assessing the risk profile of suppliers, ensuring that each operator has an appropriate multi-vendor strategy, contributing to the maintaining a diverse and sustainable 5G supply chain, or further strengthening EU capacities in the 5G and post-5G, etc. It should be emphasized, however, that these are only recommendations because national governments have their own security policies.

On the whole, cybersecurity plays a major role in the EU's digital transformation. With its Cybersecurity Act, the European Union offers a

new alternative, an approach that is fundamentally different from the American liberal or the Chinese authoritarian model. Bendiek and Schallbruck (2019) claim that the Act, which is "[e]mbedded in a policy that combines digital sovereignty with strategic interdependence" could be "the gateway to a third European pathway in cyberspace, something in between the US model of a liberal market economy and the Chinese model of authoritarian state capitalism". To some extent, the digital strategy of a country reflects the country's values and priorities. At the same time, it is one of the most essential tools in the fight for global dominance. But digital technologies are interrelated, therefore, they reach beyond the borders of single states. This also means that controlling them is an increasingly demanding task.

7. FDI Screening and Security Policy in the EU

There is one more issue that needs to be mentioned in relation with the EU's China policy. It concerns foreign direct investments in general, however, the elements including new technologies can be mainly related to China. The new EU framework for the screening of foreign direct investments entered into force in April 2019. The European Commission proposed this framework to safeguard "Europe's security and public order in relation to foreign direct investments into the Union". The list of the member states' screening mechanisms is publicly available, and it is regularly updated by the Commission. Although they vary considerably, the security dimensions of the new technologies are prominent in nearly all of them.

The list of EU screening mechanisms includes the screening mechanisms (and their amendments) of the following states: the Czech Republic, Denmark, Germany, Spain, France, Italy, Latvia, Lithuania, Hungary, Malta, the Netherlands, Austria, Poland, Portugal, Romania,

Slovenia, Slovakia, and Finland. A thorough analysis of all these states' relevant laws and their amendments would far exceed the limits of this paper; however, a representative choice of several points would suffice to have an overview of some EU countries' FDI screening.

In France, the order of 31 December 2019 relating to foreign investments entered into force. According to Article L. 151-3 of the Legislative Section of the "Monetary and Financial Code" "[f]oreign investment in any activity in France which, even if only occasionally, is part of the exercise of public authority or pertains to one of the following domains is subject to prior approval from the Minister in charge of Economy". The areas specified in the document are the following:

a) Activities likely to jeopardise public order, public safety or national defence interests.

b) Research in, and production or marketing of, arms, munitions, or explosive powders or substances.

The Regulatory Section specifies the activities relating to the exercise of public authority, and places them in the following categories: I. activities that "are likely to jeopardise national defence interests or the maintenance of public order and public safety", II. activities "that are likely to jeopardise national defence interests or the maintenance of public order and public safety, insofar as they concern infrastructure, goods or services" which have a vital role in guaranteeing the integrity, security and continuity of the energy, or water supply, or of the operation of transport networks and services, etc. The third category concerns activities "that are likely to jeopardise national defence interests, public order and public safety, when they are intended to be carried out in connection with one of the activities referred to in section I or II". These include "research and development activities relating to

critical technologies" and "research and development activities relating to the dual-use goods and technologies". The critical technologies are listed in Article 6 of the order, and they include: cybersecurity, artificial intelligence, robotics, additive manufacturing, semiconductors, quantum technologies, and energy storage.

Regarding Italy, the decree law of 15 March 2012 was complemented with "the regulation on special powers in sectors of strategic importance set forth in Articles 3 and 4-bis of the decree-law 21 September 2019, n. 105", and was converted with amendments by law November 18, 2019, n. 133. The original decree law consists of "Rules on special powers on corporate assets in the defence and national security sectors, as well as for activities of strategic importance in the energy, transport and communications sectors". The amendments available in the *Gazzetta Ufficiale* include urgent provisions concerning national cybersecurity. Most of the modifications consider the harms inflicted on national security that may derive from the malfunction, the (even partial) interruption, or the improper use of networks, information systems, and IT services. The Centre of National Assessment and Certification (CVCN), established in the Ministry of Economic Development, should be notified by the risks imposed by the supply of ICT goods, systems, or services; moreover, CVCN can carry out preliminary checks and hardware or software tests. It would be impossible to include all modifications mentioned in the document; however, there is one point that cannot be left unmentioned. It claims that international standards, i.e., the standards of the European Union were considered, referring to the EU regulation (2019/452) of the Council of Ministers.

Germany is an attractive destination for investment, therefore, the country's security risks should be regularly measured and prevented. It is the task of the Federal Ministry for Economic Affairs and Energy to

review the acquisition of German firms on a case-by-case basis. The legal framework is provided by the Foreign Trade and Payments Act and the Foreign Trade and Payments Ordinance, which include special rules that apply to the acquisitions of certain defence and IT security companies. Section 4 of the Foreign Trade and Payments Act includes the restrictions and obligations required to protect public security and external interests. Similar to their Italian counterparts, the restrictions of legal transactions and actions, and the obligations to act can be imposed "in order to implement decisions of the Council of the European Union on economic sanctions in the field of Common Foreign and Security Policy", or to implement obligations of the Member States of the European Union, UN Security Council resolutions or international agreements. Section 5 of the act specifies the subjects of restrictions, and adds that these regulations "can particularly be imposed with reference to the acquisition of domestic companies or shares in such companies by foreigners in order to guarantee essential security interests of the Federal Republic of Germany if the domestic companies: 1. manufacture or develop war weapons or other military equipment or 2. manufacture products with IT security functions to process classified state material or components essential to the IT security function of such products". These rules also apply provided these companies "have manufactured such products and still dispose of the technology if the overall product was licensed with the knowledge of the company by the Federal IT Security Agency".

So far, most EU member states have such or similar control mechanisms for foreign direct investment. As these examples show, there are tremendous differences between the different countries' acts dealing with screening FDI. The acts of several other countries which are on the list made available by the European Commission have not been amended for years, thus they do not fit exactly into the framework

provided by the EU. It is an acceptable argument that each member state has its own peculiarities concerning its security policy, still, a complete list and a more united stance on this matter would be required. Although the member states have the authority to decide whether a foreign direct investment affects their national security or public order, they should take into consideration the recommendations of the European Commission before making a final decision. None of the documents makes any specific references to China, still, the European screening framework also affects considerably Chinese investments, which already halved between 2016 and 2018 in the EU.

Rasmussen (2018) considers the EU's decision to monitor foreign investments as an important step forward, which does not obstruct trade but makes it clear that "trade and investment must be based on values and freedom, and not simply the interests of state-backed monopolies". Although he agrees with the necessity of a common position, he criticizes the European approach that only seeks to negotiate standards and rules, as opposed to the Unites States, which prefers crude action to discussion. On the whole, Rasmussen claims that "the proposal shows clearly that the EU is bringing a rule book where China brings a cheque book", therefore, the EU should move beyond this values-based approach to pursue its interests by forming "a stronger political and economic alliance with the leading Asian liberal economies". The EU published its Connectivity Strategy for Europe and Asia in September 2018, which was considered as an answer to China's Belt and Road Initiative. Among the Asian partners the relations with Japan are of particular importance, as reflected by the EU–Japan Partnership on Sustainable Connectivity and Quality Infrastructure launched in September 2019. Nevertheless, this partnership does not hinder many EU member states in pursuing their interests and continuing to favour Chinese investments.

8. Europe and the Two Technological Superpowers

Although the first steps towards developing a strong digital Europe have been taken, the EU is still far from becoming the rival of any of the two technological superpowers. On the other hand, as Bremmer (2020) observes, it has become a true regulatory superpower, which "wants to boost its own capabilities in AI while turning its strong tech regulation into a competitive advantage", since consumers trust European AI products, besides, the General Data Protection Regulation (GDPR) is "the most extensive data privacy framework in the world". He adds: "Europe doesn't have the Silicon Valley tech titans in its corner and doesn't have the state-control of capitalism to grow its own tech champions the way that Beijing has done in recent years. It also increasingly finds itself caught between Washington and Beijing's will-they-or-won't-they Cold War. Tech regulation represents Europe's best hope for resuscitating its geopolitical relevance in the 21st century" (Bremmer, 2020). This statement is acceptable; however, it should be added that even if the European Union, as a supranational organisation, has its own values, each of its member states has its own standards, too, regarding regulations and national security. Still, only a unified standpoint among members concerning technological regulation (based on European values and standards) along with joint IT research projects (coordinated at EU level) would lead to the technological emergence of the EU.

9. Conclusion

The European Digital Strategy is built on European values and individual rights. It emphasizes that Europe should have its own digital capacities, which include the protection of its citizens and businesses,

too. Security issues are of primary relevance for the EU, hence, after the implementation of the General Data Protection Regulation and the provision of a common framework for the screening of foreign direct investments, it accepted the Cybersecurity Act, which further strengthens the EU's security policy. The latter also granted new tasks to ENISA, which is enabled to prepare European cybersecurity certification schemes.

On the one hand, these developments are remarkable, moreover, they are praised by other countries, too. Countries like Japan, India, and Brazil intend to align themselves with European law because it makes more sense for globally active corporations to apply demanding EU regulations everywhere instead of operating with different standards required by different markets. On the other hand, regulations are overemphasized in the European Digital Strategy in comparison with innovation, or research and development, despite the necessity to defend European values and rights, as reflected by the first pillars of the European Commission's digital strategy, i.e., the Data Strategy and the White Paper on Artificial Intelligence. The notion of creating a single market for data will ensure data availability in the economy, and citizens as well as businesses will benefit from data driven applications. But as a common framework has been provided concerning the screening of FDI, cybersecurity, GDPR, or certification schemes, the EU should also attribute greater importance to common research initiatives, including transnational cooperation. At the same time, the organization should also rely more heavily on its talent pool, which is often lured by the two big rivals.

The steps the EU has taken so far concerning regulations and the plans to develop operating standards for European data spaces are promising. They will allow businesses, governments, and researchers to store their own data, as well as access data shared by others, which is of

crucial importance for innovation. Besides, the unified digital single market is necessary to overcome fragmentation on the digital ground.

The EU, with the diversity of knowledge and expertise represented by its member states can emerge as a technological superpower, provided these attributes are coordinated in a more effective way. Countries aspiring for membership may contribute to this common knowledge to a great extent. Only with a unified standpoint among present and future members regarding technological regulation, and with joint research projects, which are based on European values and standards, would the European Union be able to break the bipolar technological world order.

Note

* Dr Teodora Wiesenmayer received her Ph.D. in 2012 from Eötvös Loránd University, Budapest, Hungary. She holds an MA in International Relations. She was Head of International Affairs and a Senior Lecturer at Budapest Business School – University of Applied Sciences in Hungary. Her fields of research are the EU's digital strategy and its China policy. She works as an editor at Helikon Publishing. <*Email: wteo77@gmail.com*>

References

BBC News (17th May 2021). Why is Huawei Still in the UK? (Reported by Zoe Kleinman.) <*https://www.bbc.com/news/technology-57146140*>

Bendiek, Annegret and Martin Schallbruch (2019). Europe's Third Way in Cyberspace. What part does the new EU Cybersecurity Act play? *SWP Comment* 2019/C 52, 19.12.2019, 8 Seiten (doi:10.18449/2019C52). Berlin: German Institute for International and Security Affairs, Stiftung Wissenschaft und Politik (SWP). <*https://www.swp-berlin.org/10.18449/*

2019C52/>

Bremmer, Ian (2020). What happens next with Europe's new regulation of big tech. *Time*, 22nd February 2020 (Ideas). *<https://time.com/5788786/europes-new-approach-big-tech/>*

Esteban, Mario and Miguel Otero-Iglesias (2020). Washington's war on Huawei is causing angst in Madrid. *Foreign Policy*, 20th January 2020 (Argument). *<https://foreignpolicy.com/2020/01/20/spain-china-usa-washingtons-war-on-huawei-is-causing-angst-in-madrid/>*

Euractiv (19th May 2021). EU countries keep different approaches to Huawei on 5G rollout. (Reported by Oliver Noyan.) *<https://www.euractiv.com/section/digital/news/eu-countries-keep-different-approaches-to-huawei-on-5g-rollout/>*

European Union Agency for Cybersecurity (n.d.). About ENISA - The European Union Agency for Cybersecurity. *<https://www.enisa.europa.eu/about-enisa>*

European Commission (2019). List of screening mechanisms notified by Member States. *<https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157946.pdf>*

European Commission (2019). EU foreign investment screening regulation enters into force. *Press Corner*, 10th April 2019. *<https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2088>*

European Commission (2020). Secure 5G networks: Questions and Answers on the EU toolbox. *Press Corner*, 29th January 2020. *<https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_127>*

European Commission (2020). Excellence and trust in artificial intelligence. *Strategy – Priorities 2019-2024 – A Europe Fit for the Digital Age*, February 2020. *<https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en>*

European Commission (2020). The European Data Strategy – Factsheet. *Press Corner*, 19th February 2020. *<https://ec.europa.eu/commission/presscor*

ner/detail/en/fs_20_283>

European Commission (2020). Shaping Europe's digital future – Questions and Answers. *Press Corner*, 19th February 2020. *<https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_264>*

European Commission (2020). A European strategy for data. *Shaping Europe's Digital Future*, 20th March 2020. *<https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>*

European Commission (2021). The Digital Services Act package. *Shaping Europe's Digital Future*, 26th April 2021. *<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>*

Federal Ministry for Economic Affairs and Energy, Germany (2020). Investment screening. *Foreign Trade and Investment Law. <https://www.bmwi.de/Redaktion/EN/Artikel/Foreign-Trade/investment-screening.html>*

Federal Ministry of Justice and Consumer Protection, Germany. *Foreign Trade and Payments Act* of 6 June 2013 (*Federal Law Gazette* I p. 1482), as last amended by Article 4 of the Act of 20 July 2017 (*Federal Law Gazette* I p. 2789). *<https://www.gesetze-im-internet.de/englisch_awg/englisch_awg.html#p0092>*

French Treasury / FDI screening unit (2019). Order of 31 December 2019 relating to foreign investments in France. *<https://trade.ec.europa.eu/doclib/docs/2020/march/tradoc_158692.pdf>*

French Treasury / FDI screening unit (2020). *Monetary and Financial Code* – Legislative Section. *<https://trade.ec.europa.eu/doclib/docs/2020/march/tradoc_158692.pdf>*

French Treasury / FDI screening unit (2020). *Monetary and Financial Code* – Regulatory Section. *<https://trade.ec.europa.eu/doclib/docs/2020/march/tradoc_158692.pdf>*

Ministero della Giustizia (2019). *Gazzetta Ufficiale della Repubblica Italiana*, Anno 160° - Numero 272, Roma - Mercoledì, 20 novembre 2019, 29. *<https://www.gazzettaufficiale.it/eli/gu/2019/11/20/272/sg/pdf>*

Moldicz Csaba (2019). Technology transfer between China and Hungary: Opportunities and the reality in a new geopolitical environment (pp. 168-190). In: Chen Xin and Ugrósdy Márton (eds.), *China and Hungary: 70 Years of bilateral relations in a changing world*. December 2019. Budapest: China-CEE Institute.

Otero-Iglesias, Miguel (2019). Europe is not behind China and the US in 5G technology. *Elcano Blog*, 14th June 2019. Madrid: Real Instituto Elcano de Estudios Internacionales y Estratégicos (Elcano Royal Institute for International and Strategic Studies). <*https://blog.realinstitutoelcano.org/en/europe-is-not-behind-china-and-the-us-in-5g-technology/*>

Politico (17th February 2020). Vestager touts AI-powered vision for Europe's tech future. (Reported by Melissa Heikkilä.) <*https://www.politico.eu/article/margrethe-vestager-touts-ai-artificial-intelligence-powered-vision-for-europe-tech-future/*>

Politico (19th February 2020). Europe's digital vision, explained. (Reported by Laura Kayali, Melissa Heikkilä and Janosch Delcker.) <*https://www.politico.eu/article/europes-digital-vision-explained/*>

Rasmussen, Anders Fogh (2018). Time for Europe to step up its China game. *The Japan Times*, 6th November 2018 (Commentary). <*https://www.japantimes.co.jp/opinion/2018/11/06/commentary/world-commentary/time-europe-step-china-game/#.Xre3bmgzbIU*>

Reuters (22nd July 2020). Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028. (Reported by Mathieu Rosemain and Gwénaëlle Barzic.) <*https://www.reuters.com/article/us-france-huawei-5g-security-exclusive-idUSKCN24N26R*>

Segal, Adam (2019). The right way to deal with Huawei: The United States needs to compete with Chinese firms, not just ban them. *Foreign Affairs*, 11th July 2019. <*https://www.foreignaffairs.com/articles/china/2019-07-11/right-way-deal-huawei*>

Shi-Kupfer, Kristin and Mareike Ohlberg (2019). China's digital rise: Challenges for Europe. *MERICS Papers on China*, No 7 | April 2019. Berlin: Mercator Institute for China Studies (MERICS).

Slaughter, Matthew J. and David H. McCormick (2021). Data is power: Washington needs to craft new rules for the digital age. *Foreign Affairs*, May/June 2021, Vol. 100, No. 3. <*https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age*>

The New York Times (12th April 2019). Trump announces 5G plan as White House weighs banning Huawei. (Reported by Julian E. Barnes and David E. Sanger.) <*https://www.nytimes.com/2019/04/12/us/politics/trump-5g-network.html*>

von der Leyen, Ursula (2020). Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission. *Press Corner*, 19th February 2020. Brussels: European Commission. <*https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260*>

Wang, Jue (2019). The implication of global technological innovation on US–China strategic competition (pp. 15-27). In: Marianne Schneider-Petsinger, Jue Wang, Yu Jie and James Crabtree, *US–China strategic competition: The quest for global technological leadership*. November 2019. London: Chatham House (the Royal Institute of International Affairs).

Wang, Maya (2021). China's techno-authoritarianism has gone global: Washington needs to offer an alternative. *Foreign Affairs*, 8th April 2021. <*https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global*>

Yazdani, Pierre-Guive (2021). Régulation des GAFA, le réveil européen ? *Portail de l'Intelligence Économique*, 28th April 2021. <*https://portail-ie.fr/analysis/2816/regulation-des-gafa-le-reveil-europeen*>