Italy and Its Perception of the Risk of Engagement with China in R&D Projects in Science and Technology

Universiteit Leiden

Master Thesis

Leiden University

MASTER ASIAN STUDIES

East Asia Truck

Emma De Carli
Nr. 2872749
e.de.carli@umail.leidenuniv.nl

July 1, 2021

Wordcount: 14776

Supervisor:
Dr. M.G. Ferchen

Table of Contents

1. Introduction and research plan overview

The essay starts from the concerns raised by the collaboration between the Italian University of Pavia and the Chinese telecommunication company Huawei in building a lab in Pavia, Italy, for developing chips and semiconductors for wireless applications in the context of 5G, called the Microelectronics Innovation Lab. The essay begins with considering from a broader point of view Chinese investment in R&D collaborations in Europe. Then, it analyses at a country-level Italy's awareness in the discussion about Italy-China collaboration in higher education in research, in particular about technology and science cooperation. In other words, the essay is focused on trying to understand whether from a national point of view Italy has expressed any kind of perception of the possible risks in engagement with China in R&D projects in the technological sector. In doing so, I will compare some Italian official policy documents and the Italian strategy to how the government of the Netherlands has acted in protecting its country from Chinese investment in R&D. Hence, the essay will dedicate a consistent part in comparing the Italian and the Dutch approaches to Chinese investment in research. The research will be mainly based on the analysis of some Italian and Dutch primary sources. I was hoping to be able to include in my work an interview with the Italian researchers at the Microelectronics Innovation Lab, but my hopes were not fulfilled because of their unwillingness to share their thoughts and to engage in an interview. Therefore, the research is conducted only on the analysis of some primary and secondary written sources.

In order to answer the research question, I will have to give a more general introduction to the topic. First, I will place my starting point, namely this specific Sino-Italian R&D collaboration, into a more general discourse. I will start from describing China's objectives and strategy in the technological field, taking into consideration the cyber sovereignty and cyber governance discourses that take place in China. I will then explain why the recent Chinese policies in the high-tech domain have raised concern in the Western world, especially in the USA, and I will describe how the extremely politicized context we live in nowadays has developed. I will also describe not only the broader background of growing US-China technology competition and tensions, but EU-China technology cooperation and competition, too. The essay will dedicate an important part to outline the European position between the USA and China, but since the main objective of this research is Italy, I will focus more on outlining the specific context of Sino-Italian relations in terms of education cooperation. I will consider the strategy the Italian government has adopted to deal with China and with the huge amount of money it has been investing in the peninsula. As just mentioned, in order to have a more concrete view of the ongoing discussion about collaboration with China in higher education in research and to better assess Italy's position in it, I will also consider the case of the Netherlands and I will compare it to the Italian situation. In understanding how the Dutch institutions have addressed the question, I will get a clearer knowledge of different possible approaches to the discussion. I

have decided to take the Netherlands as comparative element firstly because it is the country where Leiden University is located and from which I am graduating. Secondly, because the Netherlands, as one can read in this essay, is considered an advanced and well-prepared country in terms of awareness of potential risks deriving from cooperation with China in higher education and research. This will help me in assessing Italy's situation. Finally, since I cannot speak Dutch, I have chosen the Netherlands as comparative case because of the accessibility of the Dutch sources to their English-language translated versions, which is fundamental for the comparison itself.

The aim of this study is therefore twofold. Since consciousness in EU and especially in Italy about the importance of this topic is little, first, my research aims to contribute to raise awareness about the importance of the topic for governments and for technology partners interested in engaging in relations with China. I hope my research will specifically help Italian actors face the question of how to develop safe cooperation with China, as well as how to best minimize strategic, security, and ethical risks. Second, the essay will place Italy in a broader framework and will clarify its position in the European discussion in dealing with China. Moreover, to date there is little academic literature not only about Sino-Italian research cooperation, but as well more broadly for EU-China collaboration in higher education research. With my research, I hope to reduce this existing gap. Finally, it is important to highlight that this essay does not offer policy recommendations, but only aims to be a representation of the current state of affairs.

For what concerns the sources and methods I will be using regarding the introduction part about US-China technology competition and EU-China technology cooperation and competition, I will mostly rely on previous academic publications and research. It will be fundamental as well considering primary sources, such as policy documents and official papers, both from the Chinese side but as well for the European part. Primary materials will be fundamental in the central analysis of this paper, namely assessing at a country-level analysis the Italian awareness of risks of engagement. I will analyse some important policy documents both for the Italian strategy and both for the Dutch approach in order to get the information I need and to draw my considerations about the topic.
As for my language skills, I will easily get access to both Italian language and Chinese language sources, since my mother tongue is Italian and my level of Mandarin Chinese is fluent enough to read and analyse primary sources. Primary sources will be of vital importance when considering the Italian national point of view because to date there is little literature regarding this topic. As for the Dutch part, although I cannot speak Dutch, I will find information in English, both for policy documents and for scholarly works. Articles and news will be taken in consideration as well while outlining the current situation, as well as speeches from prominent leaders.

The essay is organized as follows. The following section includes a literature review in order to situate my research within existing knowledge. I will give an introduction of China's cyber strategy and its objectives in

the technological field. I will then set foundations and outline the geopolitical and commercial debate about China-Western technological competition and about Western concerns for China's strategy. I will discuss the broader picture of the US-China decoupling and as well of the EU position of autonomy strategy in the debate. Finally, I will provide a space for some considerations about Chinese investment in R&D in Italy and some thoughts about the relations between Huawei and the University of Pavia. The third part examines the specific case of Italy-China relations starting from a broad economic point of view and then considering the educational field. I will first introduce the general Italian strategy in addressing the Chinese investment question and then the essay will follow with the analysis of some primary sources from the Italian government to assess Italy's stance in the debate. The fourth section will contain the comparison with the Dutch approach. I will first analyse some policy documents about the way the Dutch government has decided to deal with China. Then I will compare the Dutch strategy to the Italian approach and I will express some final considerations about higher research and cooperation with China. The last part will consist of a summary of the work I have been conducting and will contain some concluding thoughts that will emerge from the research about the importance of the topic and the political challenges that institutions and companies, like Huawei, are facing today.

2. Literature review

2.1. Technology as a tool of "weaponized interdependence"

It is of primary importance relying on Farrell and Newman's concept of technology as a tool of "weaponized interdependence" in order to introduce the topic (Farrell & Newman, 2019). Their discussion is based on the idea that in a globalised and interconnected world, global networks play a fundamental role in the world economy and that globalization has activated the development of "networks of interdependence", in which asymmetric growth generates networks with extreme inequality of influence. According to their definition, technology offers strategic advantages derived from one state's ability to gather information on its adversaries' intentions and tactics and to control or deny access to hubs. This therefore produces a considerable coercive power that actors can use over states or other actors. They present internet communication as an example of weaponized technology. They also claim that a states' ability to employ these forms of coercion will depend on the combination of both the structure of the network and both the domestic institutions existing in the state that is trying to make use of them. In fact, only if a state has physical or legal access over hub nodes it will be able to exploit the benefits of the weaponized interdependence and moreover, if a state is exploiting these hubs, it requires some appropriate legal and regulatory institutions. They offer the USA as an example of powerful state in which a lot of key hubs are concentrated, creating the abovementioned asymmetric network. In fact, with regards to technology numerous companies that handle and channel huge amount of global data traffic are located in the United States, like Google, Facebook, Amazon, YouTube and Twitter. One study highlights that 70 percent of global

web traffic goes through Amazon Web Services located in Northern Virginia (Freed, 2016). The same narrative applies to the semiconductor design, in which three US companies (Synopsys, Cadence, and Mentor Graphics) have the monopoly on the design of modern chips (Kleinhans, 2020). As for cyber institutions, the authority over the Internet Protocol numbers and the Domain Name System was assigned in 1998 to a private non-profit firm under California law, called the Internet Corporation for Assigned Names and Numbers (ICANN). The organisation is responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet and it is in charge of ensuring the network's stable and secure operations (ICANN Bylaws, 2019). But, although declared to be a private institution, as stated by Jospeh S. Nye, ICANN is as well at least partially accountable to the US Commerce Department, which provided the US government with a controversial implicit veto. As scholar Lu Chuanying says, "*the United States had practically complete control over formulating and managing the internet standards of all international organizations and core industries*" (Lu Chuanying, 2016).

For the past seventy years the United States has been the world's leader in technological innovation and development and has led technological and market innovation in the most recent round of economic globalization. Today, however, in a world where technological competitiveness is considered a major factor within current geopolitical tensions and systemic rivalry, the United States faces some threats to its technological leadership as well as to its economic and national security (Mcraven, Manyika & Segal, 2019). One of these challenges to the US supremacy and to the existing balance of power is represented by China and its outpacing economic growth in the last thirty years. It is a matter of fact that China's growing role in the digital domain questions not only the existing balance of geopolitical power, but also "*reshapes the rules of the game of that very system and the standards and norms underpinning it*" (Dekker & Okano-Heijmans, 2020, p. 1).

2.2. Cyber sovereignty and "technonationalism": the USA and China

The abovementioned concept of technology as a weaponized tool of interdependence can in part explain the rise of the cyber sovereignty (*wangluo zhuquan*, 网络主权) debate both in China and in Western countries. In the last twenty years policymakers and governments from every corner of the world perceive the technological and industrial sector as fundamental not only for their geopolitical strategy, but also for national security and economic competitiveness. As Evan Feigenbaum affirms, technology is seen in a strategic way that is fundamental to national security and to a successful economic competitiveness (Feigenbaum, 2019). This approach to technology and industry can be defined as "technonationalist", where governments link their national interest to supply chain security and in order to achieve it, they encourage their firms to adopt preferred standards and avoid dependence on standards set by rivals (Feigenbaum, 2019).

2.2.1. The USA

The United States is no exception to the technonationalist framework. The Trump administration has assembled a comprehensive strategy for technological competition with China which, according to Segal (2020 B), consists of disrupting chains that supply Chinese tech companies, banning transactions with them in the US and consequently restricting the outward flow of technology to China, and investing in emerging domestic technologies. In May 2019 the Trump administration issued an executive order which not only forbade American companies from supplying Huawei with components, but restricted domestic networks from using its equipment (Shepardson & Freifeld, 2019). The US reaction can be interpreted as a meaningful example of the threat perceived by the American president Trump, who reacted trying to limit the Chinese economic competitiveness in the US market and to protect the American nation from the Chinese intelligence services' surveillance and espionage. As better explained later, the US strategy was also aimed at blocking the global supplying chain, which is necessary for Chinese tech companies.

2.2.2. China

In part due to the American commercial and geopolitical defensive strategy, China has also become a technonationalist country, aiming at achieving its own cyber sovereignty. Cyber sovereignty has become a famous and frequent used word in official documents and statements released by Chinese officials since its first appearance in the 2010 White Paper outlining China's position on the Internet (SCIO, 2010). Since then, it has been repeated as a key word in both speeches held by top leaders, like for example in 2015 by General Secretary Xi Jinping himself (Xi, 2015), and in national policy documents, like in China's national cybersecurity strategy (CAC, 2016) and in its Cybersecurity Law (NPC, 2016). Using Xi Jinping words to define Chinese interpretation of cyber sovereignty, every state has the right "*to choose its online development path, its network management model and its public Internet policies, and to equal participation in international cyberspace governance".* Therefore, states should abstain from *"engaging in cyber hegemony, interfering in other countries' internal affairs, and engaging in, tolerating or supporting online activities harming the national security of other countries*" (Xi, 2015).

As Rogier Creemers explains, a more general boost for Chinese sovereignty has some historical motivations that can be traced back to the "century of humiliation" (bainian chiru, 百年 耻辱) that started in 1839 and ended in 1949, when China concept of sovereignty started to create around the idea of counteracting the presence of imperialist powers. China started to develop a feeling of distrust and a sense that foreign powers were not serious in their stated commitment to international law (Creemers, 2019). This increased during the First and Second World War, especially with the unfair treatment China felt to have received during the treaty of Versailles. This sense of distrust has not still completely disappeared today. In this way, cyber sovereignty can be interpreted as one specific manifestation of these broader tensions between China and the international arena (Creemers, 2019).

According to Adam Segal (2020 A), China pursues cyber sovereignty in order to accomplish three objectives. First, Beijing aims at maintaining a tight control over the flow of information within its national borders to ensure domestic stability, regime legitimacy, and the continued rule of the Chinese Communist Party (CCP). Second, Chinese policymakers want to foster technological self-sufficiency and independence from foreign suppliers. We must not forget that, as Rogier Creemers affirms, cyber sovereignty has not only a normative part, but a capability component as well that involves material resources linked to supply chains necessary to achieve independence (Creemers, 2019). Third, from a more geopolitical point of view, Chinese policymakers want to build their cyberspace to extend Beijing's political, military, and economic influence and counter Washington's advantages in cyberspace (Segal, 2020 A). It is clear that China is in a weak position in cyberspace, compared to the role the United States has in controlling core technologies, dominating international standards, and setting the agenda for discussions about norms of state behavior in cyberspace (Segal, 2020 A). This became particularly evident with the Snowden revelations in 2013 (Blanchard, 2015), the US technology export bans targeting ZTE and Huawei in 2018 (Segal, 2019; The Economist, 2019), and the cut-off of security support for Windows XP in 2014 (BBC, 2014; Kan, 2014). Each of these events highlighted vulnerabilities resulting from forced reliance and dependence on not only irreplaceable US technology (Creemers, 2019) but also on critical information infrastructure provided by US companies like Cisco, Microsoft, and IBM (Segal & Lan, 2016). This is one of the reasons why in 2019 Beijing has reacted by ordering every government office and public institution to remove all foreign software and hardware within three years (Yuan & Nian, 2019).

As explained, China's strategy consists of aiming at achieving its cyber sovereignty and seeking to reduce its dependence on foreign counterparts, especially from the US. In doing so, China in the last years has moved from technological purchases from Western countries to indigenous innovation (Feigenbaum, 2017) and has competed to develop semiconductors and other core technologies, as well as to diminish its vulnerability to supply chains that are closely controlled by the United States. In pursuit of this goal, Chinese leaders are mobilizing Chinese tech companies, tightening links to the countries participating in China's Belt and Road Initiative, and sustaining a campaign of cyber-industrial espionage (Segal, 2020 B). Speaking in terms of international efforts, Beijing has used its diplomatic channels to expand its concept of cyber sovereignty in multilateral organizations and forums, like the *Belt and Road Initiative* (BRI). The CCP is also using other tools of commercial diplomacy, like for example the global activities that Chinese technology firms are promoting. In fact, the CCP is also trying to mobilize private tech firms in support of national goals (Segal, 2020 B). From a domestic point of view, Beijing has developed several interlocking cybersecurity strategies, laws, measures, regulations, and standards, like for example the *Made in China 2025* project (State Council, 2015), launched in 2015 and its forthcoming follow-up *China Standards 2035* (Chipman Koty, 2020). In 2020 the National People's Congress launched a five-year plan in which

municipalities, provinces, and companies will invest about $1.4 trillion in building new infrastructure through AI, data centers, 5G, the Industrial Internet, and other new technologies (Lin, 2020).

Chinese policymakers are especially trying to reduce their country's dependence on the United States for semiconductors. In October 2019, Beijing created a $29 billion semiconductor fund, as reported by Luffy Liu (2019), and in August 2020 the Chinese State Council announced other policies to support the chip industries, including tax benefits, research and development support, and incentives for international semiconductor companies to relocate to China (State Council, 2020; Segal, 2020 B). In fact, as Cheng Ting-Fang reports for *Nikkei Asia* (2020), a couple of government-backed chip manufacturers have hired more than 100 engineers and managers from Taiwan Semiconductor Manufacturing Company, which is well-known worldwide for being the world's leading chipmaker.

As Jan-Peter Kleinhans (2019) affirms, for semiconductors China still lags behind and is still highly dependent on foreign designs, IP, and chips. More generally speaking, the semiconductor value chain is controlled by few key countries, like the United States, Taiwan, South Korea, Japan, Europe and slowly also China. It is important to specify that none of these countries has the entire production process combined in their own territories, but, in pursuit of economic efficiency, it is normal to have specialized companies on particular process steps (design, fabrication, assembly) or technologies (memory chips, processors, analog semiconductors, etc.) (Kleinhans & Baisakova, 2020). It is worth mentioning as well that no region has achieved "strategic autonomy", "technological sovereignty" or "self-sufficiency" in the semiconductor domain (Kleinhans & Baisakova, 2020). However, as said before, the US, specifically a group of US companies, has in its hands a particular production step for the electronic design automation (EDA) for semiconductors, which is the part responsible for designing any type of chip and semiconductor. Currently, and for the foreseeable future, there is no way to avoid the three US companies mentioned before (Synopsys, Cadence, and Mentor Graphics), which have the monopoly on EDA software. Therefore, if China wants to design modern chips, it must pass through one of these US companies (Kleinhans, 2020). This clearly is a huge problem for the Chinese cyber sovereignty strategy. In addition, the semiconductor industry is susceptible to these types of geoeconomic strategies like the US ban measures against Huawei in 2019, because of the very global nature of the semiconductor supply chain (Kleinhans, 2019). As Lee (2020 B) mentions, the US government cutting Huawei off from the Taiwanese firms that manufacture advanced processing chips using US-origin technology can be considered a perfect case of "weaponized interdependence", in which the US government leverages control to its firms to exert power against China and Huawei's allies.

2.3. EU's role in the debate

In this context, the European Union plays a fundamental role in China's strategy for technological innovation and leadership. Another significant aspect of China's pursuit of global technological leadership is

its trillions of foreign exchange reserves, which enable acquisitions of technological foreign companies, investment funds, direct investment overseas and R&D partnerships. As Segal affirms, in order to become more innovative, China has invested its foreign exchange reserves in "*research and development, expanded enrolment in science, technology, engineering, and mathematic disciplines at universities, and promoted research megaprojects in areas such as extra-large scale integrated circuit manufacturing, manned aerospace and moon exploration, nanotechnology, protein science, and quantum research*" (Segal, 2017). As a matter of fact, Chinese scientific R&D funding has increased by 12%–20% every year for each of the last twenty years and in 2010 China surpassed Japan as the world's second-largest investor on R&D (Segal, 2016). These commercial and political strategies for foreign direct investment (FDI) are closely linked to Europe and its important technological market.

But first of all, I will briefly introduce the European position in this China-US decoupling framework.

The European Union (EU) has historically been the most trustworthy American ally and the EU foreign policy has often been described as suffering from a "what do the Americans think syndrome" (Keukeleire & MacNaughton, 2008). Hence an alignment to the American defensive policy was expected from the EU as well. However, this did not happen. During the Trump administration many major foreign policy decisions made by Trump severely affected the transatlantic alliance, for example the US withdrawal from the Paris Agreement on climate change in 2017 (Trump, 2017) and from the Joint Comprehensive Plan of Action in 2018 (Van Schaik & Dams, 2020). Right after ex-president Trump was elected, he also famously defined Europe a "foe", with the motivation that the EU has "taken advantage" of the US and consequently created trade imbalance between the US and the EU (Contiguaglia, 2018). The foreign policy of the Trump administration has been described by Van Schaik and Dams as "*a systematic demolition not only of US foundations beneath the international order but as well of the Atlantic alliance*" (Van Schaik & Dams, 2020, p. 8). This has consecutively and inevitably led to substantial changes in the way the EU tries to place itself on the world stage. The EU has become aware that a similar approach as the US decoupling strategy is not in its interest; quite the opposite, it wants to engage and deal with China (Borrell, 2020A). The complex situation between China and the US has encouraged the EU to strive for strategic autonomy. Josep Borrell, the current EU High Representative for Foreign Affairs and Security, calls this European desire for independence his "Sinatra Doctrine", referring to his famous song *My Way*, and that he summarizes as follows: "*To avoid becoming entrenched between the US and China, the EU should deal with them in its own way: it should look at the world from its own point of view, defending its values and interests, and using the instruments of power available to it*" (Borrell, 2020 B, p. 1).

This concept of autonomy also applies to the technological field. Since there is a growing concern in Europe that EU countries are falling behind in sectors key to future economic growth and job creation, and that "*the EU should carve out its own path rather than follow those of the US or China*" (Dekker & Okano-Heijmans, 2020, p. 7), the European Commission aims at achieving technological sovereignty by

establishing European leadership in network technologies (Lee, 2020 A). As the President of the European Commission Ursula von der Leyen herself outlined in her pitch for the incoming Commission, "*it is not too late to achieve technological sovereignty in some critical technology areas*" (von der Leyen, 2019; Scott, 2019). It is not a coincidence that in 2014 the European Commission has invested EUR 700 million in research and innovation in 5G through the *Horizon 2020* project (Parlamentaire Monitor, 2015), a European funding programme, part of the *Innovation Union* initiative (Publications Office of the EU, 2016). The project is aimed at securing Europe's global competitiveness and since 2021 it has been replaced by *Horizon Europe* (Pavlovic, 2020). Moreover, the same technological sovereignty narrative is embraced by some European policymakers and governments as well, which have increasingly talked about the need for digital sovereignty to break the dominance of US and Chinese technology companies (Segal, 2020A). For example, the Gaia-X project, developed by France and Germany in 2020, would allow European countries to store their data in Europe, instead of relying on the US and the Chinese alternatives of Amazon Web Services and Alibaba (GAIA-X ,2020; Delcker & Heikkilä, 2020). The EU has started to chart its own course and in doing so has relied on Chinese investment, starting from its response to China's Belt and Road Initiative in September 2018, the launch of its Connectivity Strategy, and from the concluded negotiations with China for a Comprehensive Agreement on Investment (CAI) in the very last days of 2020 (Dekker & Okano-Heijmans, 2020).

2.4. Chinese investment in EU technology and R&D projects

Coming back to the Chinese FDI, it plays a significant role in both Chinese and European strategy. As the report by Rhodium Group and the Mercator Institute for China Studies (MERICS) affirms, while Chinese investments in the EU have decreased from EUR 18 billion in 2018 to EUR 12 billion in 2019, in 2019 ICT sector has remained the top one in terms of single transactions, accounting for 20 percent of all transactions, and came second in terms of volume with EUR 2.4 billion (Kratz et. al, 2020). They affirm that this demonstrates that Chinese firms remain interested in European technology companies and know-how and, although FDI flow has slowed down its pace over the past three years, deal-making remains strong between the two counterparts.

More important for this essay are joint R&D partnerships, which according to Rhodium Group and MERICS are currently expanding between Chinese firms and European actors (Kratz et. al, 2020). This is because R&D collaborations can provide the European involved part with significant benefits not only in terms of capital but also for creation of technologies and know-how, new products and services. As d'Hooghe and Lammertink report for *LeidenAsiaCentre* (d'Hooghe & Lammertink, 2020), in the past eight years China has allocated over 4 percent of its GDP on education every year, whereas in 2018 China's investment in R&D were around EUR 242 billion, which placed China as second in the world after to the US. The Chinese telecommunication company Huawei alone has been investing worldwide USD 600 million for R&D

partnerships in 5G technologies since 2009 (Shi-Kupfer & Ohlberg, 2019) and in Europe has research collaborations with about 150 universities (Kleinhans, 2019). However, as Rhodium Group and MERICS report, R&D collaborations could also have a long-term impact on European economic competitiveness, as they often aim at attracting or leveraging talents and technology from abroad towards China. In addition, it is not just a mere question of economic competitiveness, but also about the possible transfer of dual-use technologies to China´s military-industrial system. R&D partnership could contribute as well to enhancing the Chinese state's ability to exert mass monitoring over Chinese population.

2.5. The specificity of the Microelectronics Innovation Lab in Pavia and some general considerations

When taking into consideration Huawei's $2.24 million collaboration with University of Pavia to build the Microelectronics Innovation Lab focused on extending research into technological innovation in the field of semiconductors for wireless applications in the context of 5G over the next three to five years (Huawei, 2019), we cannot ignore the abovementioned threats reported by Rhodium Group and MERICS. As a matter of fact, if we use Rhodium Group's "green list" of trade sectors in EU-China trade relationship (Kratz, Mingey and Rose, 2020) and we place this Huawei-University of Pavia partnership, we discover that the content of this partnership can be considered as potentially sensitive, because both of the possible transfer of dual-use technology of semiconductors to China´s military system and both because of its potential contribution to improve and innovate technologies necessary for the Chinese state's ability to exert mass control over its population.

Moreover, what raises even more questions is the relations between Huawei and the Microelectronics Innovation Lab, which, as said before, has been established by both the University of Pavia and Huawei Italy. For the Huawei counterpart, the actor that is cooperating with the University of Pavia is the Huawei Milan Research Center (*Centro di Ricerca di Milano*), located in Segrate, Milan (University of Pavia, 2019; Regione Lombardia, 2019). Led by Renato Lombardi, it was established in 2008 and in Italy it plays an important role in Huawei's research and innovation sector. In 2017 Huawei conquered the primacy of the number of patents (2,398) filed at the European Patent Office (EPO), of which about 20 came from the Huawei Milan Research Center in Segrate (Biondi, 2018). As reported, the centre works with fourteen Italian universities and engages in the study of technology microwaves used in mobile and satellite communication (Biondi, 2018; Ansa, 2019). What is important to highlight is that the Huawei Milan Research Center in 2019 was added by the United States Department of Commerce to its Entity List, namely the "blacklist" that prevents those listed firms and actors from engaging in business with US counterparts (Ansa, 2019 B; Biondi, 2019). Although this move was considered political and not due to national security motivations, it still remains a significant measure that has some consequences on the Pavia case, since it is closely linked and funded by this blacklisted Huawei Milan Research Center.

What can be said about this broad topic is that it is particularly based on current events and therefore is evolving and changing every day. Governments and institutions are still figuring out what is the best strategy to adopt, given the importance and the sensitivity of the issue. I have found very challenging assessing and judging the specific case of Huawei-Pavia collaboration. I have followed what Rhodium Group in their publication "Exploring a 'Green List' for EU-China Economic Relations" (Kratz, Mingey and Rose, 2020) have built up as a framework for FDI screening in the EU. In their paper they claim that education and scientific research and development are still not considered as a key national security risk in existing EU policies, documents and official statements, and therefore they identify the education field as a green sector. Accordingly, we could consider Huawei-Pavia R&D cooperation as not controversial. However, in their report about EU imports and exports to China they dismiss critical technologies, dual-use goods, manufacture of electronic components and of communication equipment from the green list, because of military and security concerns. And therefore, the innovative semiconductors the University of Pavia is designing with Huawei can be considered as well as a possible threat. The ambiguity in evaluating the Pavia case is illustrative of a blurred situation that is still developing nowadays and is not meant to be definitive. Indeed, this vagueness can be applied to many more R&D projects in Europe and not only to this Pavia case. Although some improvements from the EU were made in terms of FDI screening regulations, what is still missing is a clear and precise understanding of how to evaluate R&D projects with Chinese firms and actors, even from academics, like Rhodium Group, and governments. As Ingrid d'Hooghe's report for *LeidenAsiaCentre* (2018) says, R&D collaborations in general are considered as a beneficial channel to improve, innovate and acquire knowledge and skills. However, cooperation not only comes with benefits but also with risks and challenges. This is mainly because the engagement of Chinese research with foreign partners is closely tied to a government strategy to develop excellent research and education that serves China's broader goal of achieving innovation and growth. This has also its roots in the Chinese 14th Five-Year Plan, formally adopted on March 11, 2021, where research is described as the foundation for scientific and technological development (State Council, 2021). The broader picture is complicated, not only because in the specific case the content in question is a dual-use technology, but because the discussions of the risks and challenges of cooperation with China in research projects is highly drenched with political concerns. This essay does not aim at condemning and judging the so-called China's "assertive" or "peaceful" intentions and does not label the Huawei-Pavia case as a threat for Italy's national and military security. However, this part of the essay wants to acknowledge the extraordinarily politicized topic, to raise concerns, to emphasize all these contradictions and the possible interpretations and to remind the reader that the general situation is complicated, nuanced, and made up by different interests and actors.

In the next section, the Italian stance in this geopolitical and technological debate will be examined. In particular, the essay will examine how the Italian government has reacted at home to this situation and to extra-EU investment, especially to China-Italy cooperation in higher education and research. After

describing the Sino-Italian relationships, the essay will focus on the analysis of some official policy documents.

3. Italy's position

3.1. Italian politics and its relationship with China

In order to briefly explain the Italian relations with China in the last few years, it is important to first mention that the Italian political background has been extremely fragmented. According to Euronews' analysis (Harris, 2016), in 2016 with Gentiloni's new government Italy has experienced its 65th government since January 1, 1946, year of the institutional referendum that led to the abandon of the monarchy in favour of the modern Italian Republic (Presidenza del Consiglio dei Ministri, B). The UK in comparison has had 25 governments over the same period. And from 2016 until nowadays Italy has seen three more changes in government led by ex-Prime Minister Giuseppe Conte (June 1st 2018 - September 4th 2019), followed by his second coalition government (September 5th 2019 - February 13th 2021) and now formed by ex-President of the European Central Bank Mario Draghi on February 13th 2021 (Presidenza del Consiglio dei Ministri). The Italian political fragmentation has indeed had significant consequences on the relation between Italy and China. In particular, with Conte's first coalition government where the political majority was composed by the far-right Northern League (*Lega Nord*) and 5 Star Movement (*Movimento 5 Stelle* - 5SM), Italy was considered having a pro-China stance (Percy, 2019). This can be explained by the fact that on March 23, 2019, Italy became the first large economy and the first G7 member to sign a Memorandum of Understanding (MoU) on China's Belt and Road Initiative (BRI) (Ansa, 2019 A), strongly sustained by 5SM leader and back then Economic and Labor Minister Luigi Di Maio. This controversial signing, although according to former PM Conte it did not question Italy's Euro-Atlantic position in any way (Fonte, 2019), has drawn wide criticism from other large Western economies, particularly those in the EU (Poggetti, 2019). Despite the fact that the intentions expressed in the MoU in 2019 did not really materialize yet, as Francesca Ghiretti (2021) says, at that time there was a positive interest in China among the Italian parliamentarians, first among all Michele Geraci. In fact, as Undersecretary of State at the Italian Ministry of Economic Development in 2018 under the first Conte administration, in 2018 Geraci was appointed to build the "China Task Force" with the aim of "*strengthening the relationship between China and Italy*" and "*guaranteeing Italy a position of leadership in Europe vis-à-vis China's Belt and Road and Made in China 2025 initiatives*" (Ministry of Economic Development, 2018). Geraci himself had strong opinions about his China-friendly approach. For example, he called for exchange of information with China in the realm of public security and he believed Chinese investments would help Italy implement the proposed tax system of universal income and flat tax (Poggetti, 2018). However, in September 2019 that government was replaced by a new coalition, which saw the 5SM being joined by the center-left Democratic Party (PD),

always led by PM Conte. This, as Lucrezia Poggetti writes in her MERICS report (2019), meant for Italy a rebalancing of relations between the EU and China and a better alignment with Brussels' coalition. This ambiguity in Italy's position can in part explain why Italy has never published any general document in which explicitly stated its approach towards the PRC and offered some recommendation to its citizens in terms of China relations, as some other EU countries have disclosed instead.[1] This rebalancing of relations between the EU and China can be seen in the proposal from some Italian parliament members in September 2019 to organize a parliamentary hearing for Hong Kong protesters (Poggetti, 2019) and, more importantly, from Italy's exercise of its "Golden Power" to scrutinize some supply deals for 5G networks, including two that involved Huawei and ZTE (Reuters Staff, 2019).

3.2. The "Golden Power"

The so-called "Golden Power" is Italy's extra-EU FDI screening regulation. It was established in 2012 and it consists of a procedure that examines foreign investment in strategic sectors and critical infrastructure in order to safeguard the assets of companies operating in areas deemed strategic and of national interest (Presidenza del Consiglio dei Ministri, A). It is controlled by the Presidency of the Council of Ministers (*Presidenza del Consiglio dei Ministri*), which is the Italian equivalent of the Prime Minister's Office. The Golden Power is therefore directly controlled by the Prime Minister themselves. As said by the Law Decree No. 21 issued on March 15, 2012 (Gazzetta Ufficiale della Repubblica Italiana, 2012), with the Golden Power the Italian government has the power to veto or impose restrictions and conditions to an investment by foreign parts in certain industries deemed strategic for the state (Gazzetta Ufficiale della Repubblica Italiana, 2012). In the Law Decree it is clearly stated that the decision is made upon objective motivation that " *make it possible to believe the existence of links between the buyer and third countries that do not recognize the principles of democracy or the rule of law, which do not respect the norms of international law or which have assumed risky behaviors towards the international community derived from the nature of their alliances or have relations with criminal or terrorist organizations or with subjects connected to them in any case*" (Gazzetta Ufficiale della Repubblica Italiana, 2012, p. 4). However, we must not forget that the decisional power is in the Prime Minister's hands and this makes any decision of foreign investment in Italy very politicized, where the state carries a certain degree of influence over these decisions.
On March 25, 2019, the Golden Power was modified expanding the critical sectors to 5G technology. With this new extension any company interested in agreements concerning the acquisition of goods or services relating to the design, construction, maintenance and management of 5G technology networks communication services, or in its components acquisition, must therefore submit a notification under the

[1] See for example the Netherlands ("The Netherlands & China: a new balance") at https://www.government.nl/documents/policy-notes/2019/05/15/china-strategy-the-netherlands--china-a-new-balance and Sweden ("Approach to matters relating to China") at https://www.government.se/legal-documents/2019/11/government-communication--20192018/

Golden Power legislation (Gazzetta Ufficiale della Repubblica Italiana, 2019). This means that any supply contract for 5G with extra-EU partners must be approved by the Prime Minister and their office. This modification of the Golden Power was called "cyber national security perimeter" (*Perimetro di sicurezza nazionale cibernetica*) and it is still taking shape. In fact, at the beginning of March 2021 a law defining in detail how to report and react to cyber attacks has been issued by the Italian government (Santarelli, 2021).

3.3. Italy's reaction to the 5G debate

The 2019 modification of the Golden Power about 5G is consistent with the 5G debate that raised in the USA and in Europe and that escalated in 2019 with the US Huawei ban. In December 2019 the Italian Parliamentary Committee for the Security of the Republic (COPA SIR, *Comitato parlamentare per la sicurezza della Repubblica*) published a document in which concerns about Huawei and ZTE were expressed. The publication ultimately called for a Huawei exclusion from the development of 5G networks in Italy (COPA SIR, 2019) and it was further enhanced in March 2020, when COPA SIR further requested that the Office of the Prime Minister adopted clearer regulations and plans to secure the development of 5G networks in Italy (Bechis, 2020). As a consequence of this discussion, Telecom Italia (TIM), the largest telecom operator in Italy, in July 2020 announced its decision to exclude Huawei from a contract for the development of its 5G networks. The decision was justified by the logic of diversification of suppliers, and therefore by a commercial reason, not a geopolitical one (Mackenzie & Pollin, 2020). This motivation was one of the elements contained in the EU's toolbox recommendations for member states. In fact, from a European point of view, the EU measures have recently picked up since January 2020 regarding the awareness about 5G risks and security problems. EU institutions published a guidelines toolbox on 5G for member states in January 2020 (European Commission, 2020 A), and later in July 2020 the EU published a report outlining progress by member states and making recommendations on issues that needed further improvement (NIS Cooperation Group, 2020). As Francesca Ghiretti says (2020), the EU reports mention Italy as a country in line with the other European nations in terms of regulatory protection for 5G. Italy is said to be well prepared in three fields: restriction of high-risk suppliers, diversity of suppliers and prohibition to outsource network centres. And if Italy is considered by the EU in line with the other European countries, it is mainly because of the 2019 extension of the 5G sector in the Golden Power.

More generally, it is worth to mention that Italy's consciousness about the sensitivity of Chinese FDI in Europe can be traced back to 2016, when Chinese FDI reached its peak. According to a report by MERICS and Rhodium group (Hanemann & Huotari, 2017), Chinese investment in Italy between 2000 and 2016 amounted to EUR 12,839 million, making it the third largest country in the EU for Chinese investment after the UK (EUR 23,633 million) and Germany (EUR 18,817 million). As just mentioned, Chinese outbound investment peaked in 2016 and this certainly contributed to the rise of awareness that the EU needed a precise tool for FDI screening. In fact, in 2017 Italy was among those European member states interested in

building a FDI screening regulation that submitted a proposal for the establishment of a framework for FDI screening (European Commission, 2017). The effective law was issued on March 21st, 2019 by the European Parliament and the Council that officially built a framework for the screening of FDI into the territory of the EU (Official Journal of the European Union, 2019). The framework became fully operational on October 11th, 2020 (Press Corner of the European Commission, 2020).

Regarding 5G, in Europe the discussion started in 2016 with the publication of an action plan for member states, in which the need for a coordinated approach was already expressed (European Commission, 2016). Later in 2019 the European Commission adopted a recommendation on cybersecurity of 5G networks (European Commission, 2019), calling on member states to complete national risk assessments, review their measures and work together on a coordinated risk assessment and a common toolbox of mitigating measures. In this European context, the Italian inclusion of 5G in its Golden Power is considered perfectly on time and coherent with EU norms.

Italy is expected to follow the EU as well as regarding the Huawei case. Although Huawei has spent some effort into its brand rehabilitation in Italy, like for example with building its third European "Cyber Security Transparency Centre" in Rome in March 2021 (Huawei, 2021), the expected trend is to see Huawei being able to access the Italian market but with limitations and controls by the Italian state and laws, especially regarding 5G networks. This can also be motivated by the fact that the current Draghi government is heavily scrutinizing foreign investment and acquisitions. As the Italian newspaper *Corriere della Sera* reports, on March 31st, 2021 the Draghi government blocked the sale of 70% of the Italian firm Lpe from the Chinese Shenzhen Invenland holdings (Massaro, 2021). Lpe is a relatively small tech firm that specializes in the epitaxial technology, necessary for the manufacture of chips and semiconductors. The decision was justified by the reason that the sale would involve an exceptional risk for public interests relating to the continuity of the supply of semiconductor electronic devices for a plurality of areas, including energy infrastructures, artificial intelligence, 5G and IoT.

3.4. R&D partnership with China in EU and in Italy: analysis of some policy documents

What is particularly important for this essay is assessing where R&D collaborations and the educational sector fit in this FDI screening framework in Italy. First of all, as mentioned before, from a broader European perspective what can be understood from Ingrid d'Hooghe's report (2018) is that the EU institutions have not yet precisely determined whether cooperation with China in higher education and research should be regulated in any way. Her paper presents the reader with both opportunities and challenges and wants to be a support for European governments and higher education institutions to openly discuss and raise awareness of the risks of Europe-China cooperation. Nowadays some evidence of awareness is slowly starting to reveal. One example is the European Commission's initiative "Tackling Foreign Interference in Higher Education Institutions and Research Organisations" (European Commission,

2020 B). Although it does not mention China directly and is still in process to be finalized, this publication in the future may provide important guidelines for all the EU member states to raise awareness and prevent foreign interference in terms of research collaborations. Another meaningful example of growing awareness in Europe is the European Research and Innovation Days (R&D Days), aimed at bringing together policymakers, researchers, entrepreneurs and the public to debate and where in their last edition in September 2020 the topic of "How to shape the future of EU-CHINA RELATIONS in R&I cooperation?" was debated.[2] Another evidence of this growing attention to the topic was the online EU-China High Level Dialogue on Research and Innovation, held on January 21, 2021 (Research and Innovation, 2021), where EU Commissioner Gabriel and the Chinese Minister for Science, Technology and Innovation Wang Zhigang discussed the progress made in research and innovation cooperation. However, to date there is no existence of any law that regulates and protects European countries in R&D cooperation with Chinese actors.

As for Italy, if we examine the Golden Power official document there is no evidence that R&D partnerships are part of this FDI screening framework. In fact, in the first general version of 2012, while the sectors of importance are identified as the energy, transport and communications ones (art. 2, clause 1, Gazzetta Ufficiale della Repubblica Italiana, 2012), the official text refers to any act or transaction from a company that involves any changes in the ownership, control or concerning any kind of merger (art. 2, clause 2, Gazzetta Ufficiale della Repubblica Italiana, 2012). Hence, the only actors that the 2012 version of the Golden Power official document involves are firms and commercial players, not universities, R&D projects and knowledge acquisition. As for the 2019 inclusion of 5G, the text refers to any stipulation of contracts or agreements concerning the purchase of goods or services related to the design, the construction, maintenance and management of 5G networks (art. 1, clause 2, Gazzetta Ufficiale della Repubblica Italiana, 2019). And therefore again, there is no reference or mention of the education field.

In terms of norms issued by the Ministry of Education, University and Research (MIUR, *Ministero dell'Istruzione, dell'Università e della Ricerca*) the category of R&D cooperation funded by international private actors is left over and does not find any space. As a matter of fact, every four years the MIUR publishes a report about the evaluation of the quality of every research project that receives or is subsidized in part by state funds.[3] A dedicated institution of the ministry exists and it is called National Agency for the Evaluation of the University and Research Systems (ANVUR, Agenzia Nazionale di Valutazione del Sistema Universitario e della Ricerca).[4] It has the only objective of assessing the quality, effectiveness and efficiency of public funding (ANVUR). However, it is not aimed at evaluating any possible

[2] For more information about this visit the dedicated EU website https://research-innovation-days.ec.europa.eu/

[3] See for example the Ministerial Decree no. 1110 of November 29, 2019 called "Linee guida per la valutazione della qualità della ricerca (VQR) 2015-2019" at https://www.miur.gov.it/web/guest/-/decreto-ministeriale-n-1110-del-29-11-2019

[4] For more information about the ANVUR institution visit https://www.anvur.it/

national, security or military risk but instead is merely a state tool that controls whether public funding that the Italian state is investing is well spent. In addition, it does not include any research project sponsored by foreign private players, as Huawei is in its relationship with University of Pavia, but it considers only projects funded by government grant.

If we look at the Ministry of Foreign Affairs and International Cooperation (MAECI, *Ministero degli Affari esteri e della Cooperazione internazionale*), there are mainly two important reports published in 2015 and in 2020 that are really similar to one another and that are both related to Italy-China cooperation in science and technology. The first one is "Science & technology: for an Italian strategy in China" (MAECI, 2015) and the second is "Italy China – Scientific and Technological Collaboration: Action Plan towards 2025" (MAECI, 2020). They both consist in a sort of guide map for Italian actors, including universities, to be guided in the Chinese point of view of technology innovation and research. As a matter of fact, the first one gives a general background about China's rise as a technological superpower and from a normative point of view pays a lot of attention to all the initiatives launched by the PRC. It even includes a list of Chinese research programmes available for Italian researchers. The second one identifies some possible areas of cooperation between China and Italy, like for example green growth and energy revolution, ICT and intelligent manufacturing. What both papers express is that they clearly follow the Chinese Five-year plans periodicity and in fact in the documents there are direct references to the 12th Plan (2011-2015) and the 13th Plan (2016-2020).[5] They both aim at creating a guideline tool for all Italian actors wishing to start or intensify their collaborations in science and technology with China. They analyse Chinese Five-year plans in terms of technology innovation, they identify Italy's strengths and strong points and try to make the two sides meet. In other words, they want to be a helpful incentive tool for Italian actors to sign successful agreements with Chinese counterparts. However, both of them convey quite the opposite meaning of this research essay, namely they encourage Italy in cooperation with China without contemplating any side effect. They do not consider any possible challenge or risk of these collaborations, even the "Action Plan towards 2025", published in 2020 in a very sensitive year for China, 5G and Huawei, does not mention any potential threat.

In conclusion, as d'Hooghe and Lammertink analyse for the *LeidenAsiaCentre* (2020), "*there are little to no signs that in Italy the politicized debate on China has resulted in concrete policy measures or documents regarding safe cooperation with China in HE&R* (Higher Education and Research)" (p. 32). The reality that is emerging is one in which R&D collaborations subsidized by private foreign actors are not controlled neither by a more general FDI screening regulation, like the Golden Power, nor by some official policy documents from the MIUR or from the MAECI. While R&D partnerships funded by the Italian state are scrutinized and

[5] For the full Chinese text of the 12th Plan visit http://www.gov.cn/2011lh/content_1825838.htm , for the English version see https://en.ndrc.gov.cn/policyrelease_8233/201612/P020191101482242850325.pdf
As for the 13th Plan Chinese full text visit http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm and for the English version see https://en.ndrc.gov.cn/newsrelease_8232/201612/P020191101481868235378.pdf

judged in terms of quality by the ANVUR, those in which the investment comes from a private company or institutions do not fall into any category. It follows that every university is responsible for its international R&D projects and that they clearly have a certain degree of freedom in choosing their partners. As analysed before, they do not have to follow any scrutiny procedure from the Italian state and because of this they possibly are an easy target or a simple way to get access to sensitive knowledge and skills.

In the following section the approach that the Dutch government has adopted to deal with foreign partnerships in research will be analysed. This will give the reader a more detailed idea of the different possible paths followed by EU countries and, while comparing the Dutch strategy with the Italian one explained earlier, I will provide the reader with a clearer understanding. As mentioned in the introductory section, the Netherlands can serve as a good comparative example mainly because, contrary to Italy, it has published some important documents that clearly state its own position in the discussion about how to interact with China in the education field as well.

4. The Netherlands and its stance

4.1. Analysis of some Dutch policy documents

As briefly mentioned before, the Dutch government in 2019 published for the first time a policy paper about the relationship with China, called "The Netherlands & China: a new balance". This policy paper reflects a reposition from a liberal and practical strategy towards China, that focused on economic interests, to an approach more conscious of the challenges that China is posing to national security and global governance (Dutch Ministry of Foreign Affairs, 2019). The paper stresses the challenges in the economic, political, and science and technology sectors and called for more cooperation between China experts and the Dutch institutions about China knowledge in the Netherlands. More specifically, the paper aims at raising awareness about challenges and risks in higher education and research cooperation with China, which are identified as political interference, lack of academic integrity, and unwanted technology transfers (Dutch Ministry of Foreign Affairs 2019). The policy paper consists in a very extensive analysis of the Sino-Dutch relations and includes sections not only about investment and trade but about sustainable cooperation in research.

First of all, the paper reflects the growing concerns about Chinese investment in the Netherlands and about China's objective of becoming a technological superpower. In particular, although the paper affirms that in terms of investment screening the "*vital Dutch sectors*" (p. 32) are generally well protected, it admits that the protection of investments and acquisitions in the 5G telecommunication sector must be strengthened. It mentions that at that time in 2019 a draft legislation - the Telecommunications (Restriction of Controlling Interests) Bill (WOZT) – was being considered to prevent undesirable controlling interests in the

telecommunications sector. This very same draft proposal was adopted in 2020 by the Dutch government and it is now called “Undesirable Control of Telecommunications Act” (Wozt). As the Italian Golden Power, the Act introduces a notification requirement compulsory to anyone who has the intention to acquire some kind of interest in a telecom party. It stipulates that a notification must be submitted to the Minister of Economic Affairs and Climate Policy, which, similarly to the Golden Power, has the power to prohibit the acquiring or holding of such controlling interest or impose a ban subject to suspensive conditions (van de Sanden & Sickinghe, 2020). The already clear situation in 2019 in the Netherlands regarding 5G and telecommunication networks was not only due to the growing concerns coming from the USA but can be traced back to 2017. As a matter of fact, in 2017 the Dutch Minister of Economic Affairs Henk Kamp was talking about safeguarding public interests, national security and public order from takeovers by foreign companies in the telecommunication sector (Government of the Netherlands, 2017).

The 2019 Dutch policy paper continues with identifying some types of Dutch interest when it comes to deal with digital espionage and risks to the Dutch national security deriving from some Chinese economic activities. Among these interests, one states that the Dutch government aims to ensure integrity and exclusivity of Dutch knowledge and information, not only of state secrets bus as well of know-how about vital processes (p. 41). This point is extremely important for the following part they discuss in the paper because this can be read as well in an education key and not only in terms of economic interests and state security.

As for the academic cooperation, the paper dedicates a whole chapter to discuss the Sino-Dutch relations when the involved parts are knowledge institutions, artists, cultural institutions and local authorities. What is significant for this essay about this chapter is the paragraph 9.1.1 “knowledge institutions”. In this section the Dutch government seems to have clearly understood the whole controversial and blurred situation between benefits and concerns about cooperation with China in education and research. In fact, they mention that, because private stakeholders, like knowledge institutions, artists and cultural institutions are not bound and controlled by any government policy, they can operate anonymously, and this can create some possible risks. Hence, the paper wants to ensure close cooperation with China on education and research and to seize the benefits of these partnerships while at the same time wants to pay sufficient attention to resolve problems and address concerns. One of these problems the Dutch government seems to have perceived is the “*risk of unwanted knowledge transfer from the Netherlands to China in areas that are of fundamental importance to the Netherlands, or that have serious consequences for the protection of Dutch or universal values or for economic or national security*” (p. 84). As an example of this they mention innovative technologies with potential dual-use applications, like semiconductors, artificial intelligence and quantum technology. Based on their analysis, their goals are to prevent these transfers of dual-use technologies and to safeguard academic freedom. The ways in which they mention to achieve this objective focus on information-sharing and coordination with Dutch players in their bilateral relationship with China

and also between central government and local and provincial authorities. In other words, they believe actors involved in research cooperation with China need to be better informed about China's policies and intentions, and to have closer coordination with other Dutch players. They intend to make communication between the Dutch government and these players easier and more frequent, so that the government can promote awareness and stakeholders can be informed frequently about government findings and policy. They also aim at encouraging and strengthening the network of contacts among these players as well at sharing information and helping each other. However, in the policy paper it is not clear how in the future they intend to realize in practical terms these objectives of strengthening cooperation and of raising awareness. The paper does not launch any kind of project regarding this topic, but this can be explained in its nature: the paper wants to be an official declaration of stance from the Dutch government and therefore focuses on a more ideological level rather than a practical one.

Another extremely important document necessary to assess the Dutch perspective in the risk of engagement with China in research and education is the "Checklist for Collaboration with Chinese Universities and Other Research Institutions" (Bekkers, Oosterveld & Verhagen, 2019), published by *The Hague Centre for Strategic Studies* in 2019 and specifically commissioned by the Dutch government. The report can be considered as the foundation for the 2019 policy document "The Netherlands & China: a new balance" because it consists of a description of the dynamics with which cooperation between universities and Chinese counterparts develops. The research is extremely reality-based in its nature and this is what makes the publication useful and interesting for policymakers. The study, in fact, was based on several interviews with scientists and university staff in the Netherlands and abroad who have first-hand experience of working with China, including some Chinese researchers as well. The essay does not only focus on the Netherlands, but research was also conducted in Poland, Germany and Denmark. Interviews were organized according to ten questions that investigate the matter. Examples of questions are: why working with a Chinese partner, who will fund the partnership and how this will affect the project, what kind of form does the cooperation have, who can use and get access to the findings of the joint research, if limitations and censorship on academic freedom is expected, whether the management of data is compliant with privacy regulations and to what extent employees or others involved in the partnership could be exposed to risks of a political nature. Of course, different answers to these questions will implicate different kinds of R&D projects and different risks of engagement from the Dutch counterpart. What I would like to highlight from this paper is the sixth question (p. 7), which goal is to understand among the interviewees whether the participants understand the potential risks and if they know about precautions that have been taken. The research affirms that "*in general, researchers with experience in China say that Western institutions have not built up sufficient awareness of the risks of working with Chinese partners*" (p.8). It continues saying that, since some institutions are conscious of this lack of protection from a government level, they have created their own set of regulations and guidelines. The paper mentions as an

example the Netherlands Organisation for Applied Scientific Research (TNO), which is the independent research agency that connects public and private organizations and companies to knowledge in order to create innovations.[6] The TNO has recently decided to not admit Chinese partners to projects that develop new technology and as a form of protection every member of the TNO staff has to undergo some security checks. Indeed, the same prevention norms are not expected from other players and the Dutch government is well aware of this. It recognizes the autonomy of higher education and research institutions and it acknowledges that they are not bound to government rules and therefore can potentially sign R&D agreements that could not respect the strategy the Dutch government is adopting.

4.2. Comparison between Italy and the Netherlands

If we compare the Dutch approach we have just now analysed to the Italian strategy discussed in the previous section, we will notice that from a government level these two realities share some similarities but at the same time show important differences in their approaches.

From what we can see from a point of view of FDI screening regulation, both countries share the same logic of regulatory protection. In fact, they have developed official policy documents to protect from foreign acquisitions that could threaten their national security. This is especially true for telecommunication investments from extra-EU investors. This is valid for Italy, that in 2019 adopted the new modification the Golden Power called "cyber national security perimeter", and for the Netherlands as well, that in 2020 issued its "Undesirable Control of Telecommunications Act" (Wozt). However, if we move away from a commercial and economic point of view in favour of a perception of risks of engagement, specifically in higher education and research cooperation, the situation becomes a little bit different. What is emerging from the analysis of the Dutch documents is that the government of the Netherlands is conscious of both benefits and challenges that derive from cooperation with China in the education field. In fact, as explained before, both the documents "The Netherlands & China: a new balance" and "Checklist for Collaboration with Chinese Universities and Other Research Institutions" reflect the deep level of awareness the government has about the topic. While stressing the importance of cooperating with China on research projects, it also recognizes the need to take initiatives to raise awareness and provide support to academia. As d'Hooghe and Lammertink say in their report for LeidenAsiaCentre (2020), the Dutch Minister of Foreign Affairs has published manuals for academia on export control regulations and has organised seminars on the topic to sensitize its players (d'Hooghe & Lammertink, 2020). It may not have issued any regulations that would control and regulate R&D agreements with foreign investors, but the publication of the policy document "The Netherlands & China: a new balance" remains an important official standpoint that marks and defines the Dutch position in the debate. The fact that the Dutch government has slowly started to

[6] For more information about the Netherlands Organisation for Applied Scientific Research (TNO), visit the website https://www.tno.nl/en/

organize such events to promote awareness is in line not only with the objectives they clarify in their policy document, but as well with the practical suggestions that *The Hague Centre for Strategic Studies* was proposing in its "Checklist for Collaboration with Chinese Universities and Other Research Institutions" in its last part called "briefing" (p. 14). In this part, in fact, the authors suggest that those involved in relations with China should be informed and trained about China before starting their contacts with China and also after the end of their experience in order to check if any potential risks actually emerged and to identify possible patterns.

Italy, on the other hand, does not seem to have developed this such degree of consciousness. From the analysis of the policy documents in the third section, like the "Italy China – Scientific and Technological Collaboration: Action Plan towards 2025" document published by the MAECI, what can be read is that these papers want to encourage Italian companies in creating and in strengthening collaborations with China. They consist in guidelines to follow to reach beneficial agreements with the Chinese counterpart and to gain economic advantages from it. As mentioned before, they analyse the Chinese technological strategy that the CCP has adopted throughout the years through its several Five-Year Plans and they try to make a way for Italian firms and business in China. They do not warn the reader about possible risks. Especially for technology and innovation, they do not consider any potential risk or challenge deriving from these partnerships. They do not convey any sense of threat and they do not present the reader with any warning or knowledge about the ways in which scientists, researchers and firms working with China could be approached or influenced or about how the Chinese counterpart could act. In this way the documents analysed before demonstrate to lack a sense of awareness about the challenges and risks of engagement with China. Therefore, compared to the Dutch policy documents presented before, the Italian ones can be considered the polar opposite in terms of level of awareness.

Another curious worth-mentioning note about the Italian situation is the contradiction raising from the awareness visible in the establishment of the modification of the Golden power called "cyber national security perimeter" in 2019 and the completely absence of consciousness in the two documents published by MAECI in 2015 and in 2020. Although part of different ministries, the Golden Power and the two documents by MAECI are all issued by the same institution, namely the Italian government, and therefore should reflect a uniform and consistent approach to the Sino-Italian discussion. However, this is not the case. If on one hand the Golden Power and its modification about 5G and telecommunication supply contracts in 2019 can convince the reader that the Italian government is aware of the threat China is representing nowadays as a technological power, on the other hand the documents by MAECI prove the opposite. In the Golden Power the image of China we are offered is one of a dangerous superpower that could pose some significant risks for other countries' national security and whose technological rise must be monitored. In the two MAECI documents China is depicted as a booming technological partner from whose collaboration the Italian counterpart can greatly benefit. Although this essay does not aim at

investigating the reasons laying behind this contradiction, one of the possible explanations for the Italian government not considering cooperation with China in business and higher education and research as alarming may be the political fragmentation that has characterized Italy in the last recent years. This political discontinuity may have not given sufficient foundation for some kind of stability and consistency in terms of strategy towards China.

5. Conclusion

In conclusion, as analysed earlier, at a European level nowadays there is no existence of a FDI screening regulation that includes the field of research cooperation, nor any specific guideline for cooperation with China in higher education and research is available. However, throughout Europe some little signs of awareness about the importance of regulating and protecting R&D projects are gradually starting to reveal. As mentioned before, the European Commission's not yet finalized initiative "Tackling Foreign Interference in Higher Education Institutions and Research Organisations" (European Commission, 2020 B) could be in the future a good starting point for building some kind of productive discussion. Moreover, European Research and Innovation Days (R&D Days) and some high-level dialogue between EU politicians are slowly laying the foundation for the matter to be discussed and to be brought to the attention of politicians and policymakers.

Despite the absence of any regulatory framework and any guidelines, some EU countries have acted independently and have published some roadmaps for developing sustainable collaboration with China. These are Germany, the Netherlands, the UK and Sweden. Among them, the Dutch government in its 2019 document "The Netherlands & China: a new balance" seems to have clearly understood the controversial and blurred situation between benefits and concerns about collaboration with China in education and research, as it wants to promote cooperation between Dutch actors and the Dutch government in order to raise awareness about the potential risks of engagement with China. However, we must not forget that none of these guidelines published by European countries, including the Dutch documents, is prescriptive. They can assist institutions, players and actors in making decisions concerning China, they can initiate a conversation about sustainable partnership with stakeholders within higher education and research institutions in a country and they can help in estimating the risks in cooperation with China. But they do not act as reglementary framework in which the players can move and build agreements. They all intend to stimulate and support these institutions in developing their own regulation frameworks, not to decide for and control them.

Italy in this context is a controversial country characterized by some contradictions. The awareness about the importance of 5G telecommunication supply contracts and acquisitions becomes evident when

analysing the Golden Power and its text. From an economic point of view, the Italian government identifies extra-EU investments and acquisitions as potential threats to its national security. However, from what has emerged in the comparison with the Dutch China approach, it does not regard investments from foreign actors in Italian R&D projects as a danger, not for ethical motivations, nor for military concerns, nor for reasons of national security or of economic competitiveness. Instead, from the analysis of the documents published by MAECI, Italy considers Chinese investment in the scientific and technological sector as a great opportunity for economic development and growth of profits. Indeed, this is a considerable part when engaging with China, but it must not be the only side of the coin that we consider. As the Dutch documents analysed before have expressed, at a government level it is important to recognize both benefits and challenges that derive from cooperation with China, especially in the education field which is still not regarded as a potential source of threat. It is also fundamental to acknowledge the need to take initiatives to raise awareness and provide support to academia with regard to compliance issues.

As *The Hague Centre for Strategic Studies* (Bekkers, Oosterveld & Verhagen, 2019) stresses in its conclusion, what is important in the context of higher education and research cooperation is not only to recognize and to become aware of the challenges China is imposing to European countries, but also to understand whose responsibility is to deal with them and to protect the players involved in the game. While the Dutch government seems to have reached some sense of awareness in setting standards and in safeguarding its interests, Italy seems to be far away from this. At a more general level, the EU and every European government should clearly determine whether it must be a government responsibility or if it must be left to the private stakeholders to decide for themselves.

Finally, I would like to make some general considerations about my inability of engaging with the Microelectronics Innovation Lab in an interview. As explained by d'Hooghe and Lammertink, compared to the situation in 2018, "*today's HE&R collaboration takes place in a political climate where many are far more critical of Chinese policies and behaviour*" (d'Hooghe & Lammertink, 2020, p. 21) and where institutions involved in cooperation with China in education and research are "*increasingly alarmed by incidents involving Chinese scholars, students, and the Chinese government*" (p.21). Huawei in particular, after the Huawei ban by the US president Trump in May 2019, has found itself in the eye of an extremely politicized storm and since then has been acted to contain the damage and to restore its brand. Institutions and companies like Huawei are inevitably influenced by the decoupling debate and the cyber sovereignty discussion. They are still trying to understand how to act and how to remain as less politicized as possible in this highly sensitive context. This can in part explain the reason why taking part in an interview would have put them in a potentially difficult situation. However, although Donal Trump was not re-elected in 2020, this politicized debate does not seem to be over yet; quite the opposite, it is expected to heighten. We are expecting to move towards a future where companies working in the telecommunications sector will be

more controlled and where higher education and research institutions will be supervised by some kind of government regulations.

6. Bibliography

ANVUR (National Agency for the Evaluation of the University and Research Systems): Missione, https://www.anvur.it/anvur/missione/

Ansa (2019 A). Conte: da Via della Seta benefici a Italia e Cina. *Ansa.it*. March 22, 2019. https://www.ansa.it/sito/notizie/politica/2019/03/22/via-seta-conte-da-memorandum-benefici-a-italia-e-cina_464a365f-5c47-447d-929f-b8f4f7013bdd.html

Ansa (2019 B). In lista nera Usa anche Huawei Italia e centro di Milano. *Ansa.it.* August 21, 2019. https://www.ansa.it/sito/notizie/tecnologia/tlc/2019/08/21/in-lista-nera-usa-anche-huawei-italia-e-centro-milano-_1269937b-b608-44f0-8740-3c4da901bf42.html

BBC (2014). Windows 8 a 'threat' to China's security. June 5, 2014. https://www.bbc.com/news/technology-27712908

Bechis, F. (2020). Huawei e 5G, ecco come (e perché) Volpi richiama Conte in Copasir. *Formiche*. March 3, 2020. https://formiche.net/2020/03/5g-volpi-conte-copasir/

Bekkers, F.; Oosterveld, W. & Verhagen, P (2019). Checklist for Collaboration with Chinese Universities and Other Research Institutions. *The Hague Centre for Strategic Studies*. January 31, 2019. https://hcss.nl/report/checklist-for-collaboration-with-chinese-universities-and-other-research-institutions/

Biondi, A. (2018). È a Segrate il «cervello» di Huawei, qui nasce la gran parte dei suoi brevetti. *Il Sole 24 Ore.* April 2, 2018. https://www.ilsole24ore.com/art/e-segrate-cervello-huawei-qui-nasce-gran-parte-suoi-brevetti--AEUkrcQE

Biondi, A. (2019). Huawei, nella lista nera Usa anche il centro ricerche di Segrate. *Il Sole 24 Ore*. August 21, 2019. https://www.ilsole24ore.com/art/huawei-lista-nera-usa-anche-centro-ricerche-segrate-ACyT5Zf

Blanchard, B. (2015). Snowden revelations just gave China more ammunition against US hacking. *Business Insider*. April 20, 2015. https://www.businessinsider.com/r-china-seriously-concerned-at-new-zealand-hack-attempt-report-2015-4?international=true&r=US&IR=T

Borrell, J. (2020 A). China, the United States and us. European External Action Service. July 31, 2020. https://eeas.europa.eu/headquarters/headquarters-homepage/83644/china-united-states-and-us_en

Borrell, J. (2020 B). The Sinatra Doctrine. How the EU Should Deal with the US–China Competition. Istituto Affari Internazionali. September 2020. https://www.iai.it/en/pubblicazioni/sinatra-doctrine-how-eu-should-deal-us-china-competition

CAC (Cyberspace Administration of China) (2016). Guojia wangluo kongjian anquan zhanlüe (国家网络空间安全战略) [National Cyberspace Security Strategy]. December 27, 2016. http://www.cac.gov.cn/2016-12/27/c_1120195926.htm Transaltion available at: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

Cheng, T. (2020). China hires over 100 TSMC engineers in push for chip leadership. *Nikkei Asia*. August 12, 2020. https://asia.nikkei.com/Business/China-tech/China-hires-over-100-TSMC-engineers-in-push-for-chip-leadership

Chipman Koty, A. (2020). What is the China Standards 2035 Plan and How Will it Impact Emerging Industries?. *China Briefing*. July 2, 2020. https://www.china-briefing.com/news/what-is-china-standards-2035-plan-how-will-it-impact-emerging-technologies-what-is-link-made-in-china-2025-goals/

Contiguaglia, C. (2018). Trump: EU is one of United States' biggest foes. *Politico*. July 15, 2018. https://www.politico.eu/article/donald-trump-putin-russia-europe-one-of-united-states-biggest-foes/

COPA SIR (2019). Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale. December 12, 2019. https://parlamento18.camera.it/228

Creemers, R. (2019). China's Conception of Cyber Sovereignty: Rhetoric and Realization. SSRN. February 5, 2019. https://ssrn.com/abstract=3532421 or http://dx.doi.org/10.2139/ssrn.3532421

d'Hooghe, I. et al. (2018). Assessing Europe-China Collaboration in Higher Education and Research. *LeidenAsiaCentre*. 2018. https://leidenasiacentre.nl/wp-content/uploads/2018/11/LeidenAsiaCentre-Report-Assessing-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf

d'Hooghe, I. & Lammertink, J. (2020). Towards Sustainable Europe-China Collaboration in Higher Education in Research. *LeidenAsiaCentre*. October 2020, https://leidenasiacentre.nl/towards-sustainable-europe-china-collaboration-in-higher-education-and-research/

Dekker, B. & Okano-Heijmans, M. (2020). Dealing with China on high-tech issues. Clingendael Netherlands Institute of International Relations. December 22, 2020. https://www.clingendael.org/publication/dealing-china-high-tech-issues

Delcker, J. & Heikkilä, M. (2020). Germany, France launch Gaia-X platform in bid for 'tech sovereignty'. *Politico.* June 4, 2020. https://www.politico.eu/article/germany-france-gaia-x-cloud-platform-eu-tech-sovereignty/

Dutch Ministry of Foreign Affairs (2019). The Netherlands & China: a new balance. May 15, 2019. https://www.government.nl/documents/policy-notes/2019/05/15/china-strategy-the-netherlands--china-a-new-balance

European Commission (2016). 5G for Europe: An Action Plan. September 14, 2016. https://digital-strategy.ec.europa.eu/en/library/communication-5g-europe-action-plan-and-accompanying-staff-working-document

European Commission (2017). Proposal for a regulation of the European Parliament and of the Council establishing a framework for screening of foreign direct investments into the European Union. September 9, 2017. https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-487-F1-EN-MAIN-PART-1.PDF

European Commission (2019). Commission Recommendation on Cybersecurity of 5G networks. March 26, 2019. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks

European Commission (2020 A). The EU Toolbox for 5G Security. January 29, 2020. https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

European Commission (2020 B). Concept Note on Tackling Foreign Interference in Higher Education Institutions and Research Organisations. February 20, 2020 available at https://s3.eu-central-1.amazonaws.com/euobs-media/3ef6dc3d60ee27a2df16f62d47e93fdc.pdf

Farrell, H. & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*. Volume 44, Number 1. Summer 2019. pp. 42-79

Feigenbaum, E. (2017). The Deep Roots and Long Branches of Chinese Technonationalism. *The Carnegie Endowment for International Peace.* August 12, 2017. https://carnegieendowment.org/2017/08/12/deep-roots-and-long-branches-of-chinese-technonationalism-pub-72815

Feigenbaum, E. (2019). In Asia, Disruptive Technonationalism Returns. *The Carnegie Endowment for International Peace*. November 13, 2019. https://carnegieendowment.org/2019/11/13/in-asia-disruptive-technonationalism-returns-pub-80331

Fonte, G. (2019). Conte, accordo con Cina non mette in dubbio alleanza euro-atlantica Italia. *Reuters*. March 19, 2019. https://cn.reuters.com/article/cina-italia-conte-idITKBN1R01AH-OITTP

Freed, B. (2016). 70 Percent of the World's Web Traffic Flows through Loudoun County. *Washingtonian.* September 14, 2016. https://www.washingtonian.com/2016/09/14/70-percent-worlds-web-traffic-flows-loudoun-county/

GAIA-X: A Federated Data Infrastructure for Europe (2020). https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

Gazzetta Ufficiale della Repubblica Italiana (2012). DECRETO-LEGGE 15 marzo 2012, n. 21. March 15, 2012. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2012-03-15;21!vig=

Gazzetta Ufficiale della Repubblica Italiana (2019). DECRETO-LEGGE 25 marzo 2019, n. 22. March 25, 2019. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2019-03-25;22!vig=

Ghiretti, F. (2020). Europe's Manoeuvring on 5G Technology: The Case of Italy. Istituto Affari Internazionali. September 24, 2020. https://www.iai.it/en/pubblicazioni/europes-manoeuvring-5g-technology-case-italy

Ghiretti, F. (2021). The Belt and Road in Italy: 2 Years Later. *The Diplomat*. March 23, 2021. https://thediplomat.com/2021/03/the-belt-and-road-in-italy-2-years-later/

Government of the Netherlands (2017). National government seeks legal conditions for takeovers in the telecom sector. February 2, 2017. https://www.government.nl/latest/news/2017/02/16/national-government-seeks-legal-conditions-for-takeovers-in-the-telecom-sector

Hanemann, T. & Huotari, M. (2017). Record flows and growing imbalances: Chinese investment in Europe in 2016. Rhodium Group and MERICS. January 03, 2017. https://merics.org/en/report/record-flows-and-growing-imbalances-chinese-investment-europe-2016

Harris, C. (2016). Why do governments in Italy change so often?. *Euronews*. December 13, 2016. https://www.euronews.com/2016/12/13/why-do-italian-governments-change-so-often

Huawei (2019). Huawei continua a investire in Italia, annunciato il Microelectronics Innovation Lab realizzato in collaborazione con l'Università di Pavia. July 15, 2019. https://e.huawei.com/it/news/it/2019/20190715_Huawei_Microelectronics_Innovation_Lab

Huawei (2021). Huawei inaugura a Roma il suo 'Cyber Security Transparency Centre'. March 3, 2021. https://e.huawei.com/it/news/it/2021/20210323_Huawei_Cyber_Security_Transparency_Centre_Roma

ICANN Bylaws (2019): https://www.icann.org/resources/pages/governance/bylaws-en . November 28, 2019.

Kan, M. (2014). China bans government purchases of Windows 8, surprising Microsoft. PCWorld. May 20, 2014. https://www.pcworld.com/article/2157220/china-bans-government-purchases-of-windows-8-surprising-microsoft.html

Keukeleire, S. & MacNaughton, J. (2008). The Foreign Policy of the European Union. *Houndmills: Palgrave Macmillan.*

Kleinhans, J. (2019). Europe's 5G challenge and why there is no easy way out. *Technode.* June 25, 2019. https://technode.com/2019/06/25/europes-5g-challenge-and-why-there-is-no-easy-way-out/

Kleinhans, J. (2020). TSMC prepares for US-China chips decoupling. *Technode*. May 27, 2020. https://technode.com/2020/05/27/tsmc-prepares-for-us-china-chips-decoupling/

Kleinhans, J. & Dr. Baisakova, N. (2020). The global semiconductor value chain. *Stiftung Neue Verantwortung*. October 2020. https://www.stiftung-nv.de/de/publikation/global-semiconductor-value-chain-technology-primer-policy-makers

Kratz, A. et. al. (2020). Chinese FDI in Europe: 2019 Update. Rhodium Group and MERICS. April 2020. https://merics.org/en/report/chinese-fdi-europe-2019-update

Kratz, A.; Mingey, M. and Rose, D. (2020). Exploring a 'Green List' for EU-China Economic Relations. Rhodium Group. September 29, 2020. https://rhg.com/research/green-list/

Lee, J. (2020 A). 5G and Huawei: Europe grapples with risk. MERICS. February 18, 2020. https://merics.org/en/analysis/5g-and-huawei-europe-grapples-risk

Lee, J. (2020 B). US campaign against Chinese vendors: The Global 5G Contest Escalates. MERICS. August 6, 2020. https://merics.org/en/analysis/us-campaign-against-chinese-vendors-global-5g-contest-escalates

Lin, L. (2020). China's Trillion-Dollar Campaign Fuels a Tech Race With the U.S. . *The Wall Street Journal.* June 11, 2020. https://www.wsj.com/articles/chinas-trillion-dollar-campaign-fuels-a-tech-race-with-the-u-s-11591892854?mod=hp_listb_pos3

Liu, L. (2019). China's 'Big Fund' Phase II Aims at IC Self-Sufficiency. *EE Times*. October 30, 2019. https://www.eetimes.com/chinas-big-fund-phase-ii-aims-at-ic-self-sufficiency/

Lu, C. (2016). Wangluo kongjian guoji guize tixi yu Zhong Mei xinxing daguo guanxi (网络空间国际规则体系与中美新型大国关系) [The International Cyberspace Rule-Based System and the China-U.S. New Type of Great-Power Relations]. *People's Daily*. Theory Channel. December 2, 2016. http://theory.people.com.cn/n1/2016/1202/c386965-28920732.html

Mackenzie, J. & Pollin, E. (2020). Huawei says it's working with Telecom Italia despite 5G exclusion: paper. *Reuters*. July 20, 2020. https://www.reuters.com/article/us-huawei-italy/huawei-says-its-working-with-telecom-italia-despite-5g-exclusion-paper-idUSKCN24L0IM

MAECI (Ministry of Foreign Affairs and International Cooperation) (2015). Scienza & tecnologia: per una strategia italiana in Cina. June 13, 2015. https://www.esteri.it/mae/en/sala_stampa/archivionotizie/approfondimenti/2015/06/scienza-tecnologia-per-una-strategia.html and https://www.esteri.it/mae/resource/doc/2015/06/studio_cina_final.pdf

MAECI (Ministry of Foreign Affairs and International Cooperation) (2020). Italia Cina – Collaborazione Scientifica e Tecnologica: Piano d'Azione verso il 2025. March 20, 2020. https://www.esteri.it/mae/it/sala_stampa/archivionotizie/approfondimenti/italia-cina-collaborazione-scientifica-e-tecnologica-piano-d-azione-verso-il-2025.html

Massaro, F. (2021). Draghi ferma i cinesi con il «golden power»: cos'è e perché l'italiana Lpe è stata protetta. *Corriere della Sera*. April 9, 2021. https://www.corriere.it/economia/aziende/21_aprile_09/draghi-ferma-cinesi-il-golden-power-cos-e-perche-l-italiana-lpe-stata-protetta-ec7b7088-98fa-11eb-9898-68a50e5b3d06.shtml

Mcraven, W.; Manyika, J. & Segal, A. (2019). America faces fresh challenges to technology innovation leadership. *The Hill*. September 19, 2019. https://thehill.com/opinion/technology/461958-america-faces-fresh-challenges-to-technology-innovation-leadership

Ministry of Economic Development (2018). Italy's Ministry of Economic Development Launches Task Force China. August 21, 2018. https://www.mise.gov.it/index.php/en/news/2038554-italy-s-ministry-of-economic-development-launches-task-force-china

Mueller, M. L. (2009). Ruling the Root: Internet Governance and the Taming of Cyberspace. Cambridge Mass.: *MIT Press.* 2009.

NIS Cooperation Group (2020). Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity. July 24, 2020. https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

NPC (National People's Congress) (2016). Zhonghua renmin gongheguo wangluo anquan fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China]. November 7, 2016. http://www.cac.gov.cn/2016-11/07/c_1119867116.htm Translation available at: https://chinacopyrightandmedia.wordpress.com/2016/11/07/cybersecurity-law-of-the-peoples-republic-of-china/

Nye, J. S. (2014). The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance Paper Series, 1. 2014.

Official Journal of the European Union (2019). Regulation (EU) 2019/452. March 21, 2019. http://data.europa.eu/eli/reg/2019/452/oj

Parlamentaire Monitor (2015). The EU and China signed a key partnership on 5G, our tomorrow's communication networks. September 28, 2015. https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vjxp9fit0wwh?ctx=vh87km1jz6v2&tab=1&start_tab0=60

Pavlovic, E. (2020). Horizon Europe: introducing the EU's new framework programme. *LabsExplorer*. March 9, 2020. https://www.labsexplorer.com/c/horizon-europe-introducing-the-eu-s-new-framework-programme_211

Percy, J. (2019). Why Is Italy's Government Considered Pro-China?. *China Briefing.* June 17, 2019. https://www.china-briefing.com/news/italy-government-china-belt-and-road/

Poggetti, Lucrezia (2018), "Italy charts risky course with China-friendly policy", MERICS, October 11, 2018, https://merics.org/en/analysis/italy-charts-risky-course-china-friendly-policy

Poggetti, L. (2019). Italy's new government lays the foundation for a more balanced China policy. MERICS. September 17, 2019. https://merics.org/en/analysis/italys-new-government-lays-foundation-more-balanced-china-policy

Presidenza del Consiglio dei Ministri (A): Golden Power. http://www.governo.it/it/dipartimenti/dip-il-coordinamento-amministrativo/dica-att-goldenpower/9296

Presidenza del Consiglio dei Ministri (B): I Governi nelle Legislature. https://www.governo.it/it/i-governi-dal-1943-ad-oggi/i-governi-nelle-legislature/192

Press Corner of the European Commission (2020). EU foreign investment screening mechanism becomes fully operational. October 9, 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1867

Publications Office of the EU (2016). State of the innovation union 2015. July 1, 2016. https://op.europa.eu/en/publication-detail/-/publication/0487b7b9-b5d6-11e5-8d3c-01aa75ed71a1/language-en/format-PDF/source-71238593

Regione Lombardia (2019). Alleanza Huawei-Università, parte laboratorio di ricerca da 1,7 milioni di dollari. Redazione Open Innovation. August 28, 2019. https://www.openinnovation.regione.lombardia.it/it/b/572/alleanzahuaweiuniversitpartelaboratoriodiricercadamilionididollari

Research and Innovation (2021). EU-China High Level Dialogue on Research and Innovation. January 25, 2021. https://ec.europa.eu/info/news/eu-china-high-level-dialogue-research-and-innovation-2021-jan-25_en

Reuters Staff (2019). Italy approves use of special powers over 5G supply deals. *Reuters*. September 5, 2019. https://www.reuters.com/article/us-huawei-tech-5g-italy/italy-approves-use-of-special-powers-over-5g-supply-deals-idUSKCN1VQ1YG

Santarelli, M. (2021). Perimetro nazionale cibernetico: approvato il secondo DPCM, ma c'è ancora tanto da fare. *Cybersecurity 360.* March 5, 2021. https://www.cybersecurity360.it/cybersecurity-nazionale/perimetro-nazionale-cibernetico-approvato-il-secondo-dpcm-ma-ce-ancora-tanto-da-fare/

SCIO (The State Council Information Office) (2010). The Internet in China (White Paper). June 8, 2010. http://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm

Scott, M. (2019). What's driving Europe's new aggressive stance on tech. *Politico*. October 27, 2019. https://www.politico.eu/article/europe-digital-technological-sovereignty-facebook-google-amazon-ursula-von-der-leyen/

Shi-Kupfer, K. & Ohlberg, M. (2019). China's Digital Rise. MERICS. April 8, 2019. https://merics.org/en/report/chinas-digital-rise

State Council (2015). Guowuyuan guanyu yinfa "zhongguo zhizao 2025" de tongzhi (国务院关于印发《中国制造 2025》的通知) [Notice of the State Council on "Made in China 2025"]. May 19, 2015. http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm

State Council (2020). Guowuyuan guanyu yinfa xin shiqi cujin jicheng dianlu chanye he ruanjian chanye gao zhiliang fazhan ruogan zhengca de tongzhi (国务院关于印发新时期促进集成电路产业和软件产业高质量发展若干政策的通知) [The State Council's Issues Concerning the Promotion of Integrated Circuit Industry and notice of several policies for the high-quality development of the software industry]. August 4, 2020. http://www.gov.cn/zhengce/content/2020-08/04/content_5532370.htm

State Council (2021). Zhonghua renmin gongheguo guomin jingji he shehui fazhan di shisi ge wu nian guihua he 2035 nian yuanjing mubiao gangyao (中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要) [The Fourteenth Five-Year Plan for the National Economic and Social Development of the People's Republic of China and the Outline of the Long-term Goals for 2035]. March 13, 2021. http://www.gov.cn/xinwen/2021-03/13/content_5592681.htm

Segal, A. (2016). Why China Hacks the World. *Christian Science Monitor*. January 31, 2016. https://www.csmonitor.com/World/Asia-Pacific/2016/0131/Why-China-hacks-the-world

Segal, A. & Lan, T. (2016). Reducing and Managing U.S.-China Conflict in Cyberspace. *The National Bureau of Asian Research*. Special Report no. 57, pp. 43-61. April 2016. https://www.nbr.org/publication/reducing-and-managing-u-s-china-conflict-in-cyberspace/

Segal, A. (2017). How China is preparing for cyberwar. *Christian Science Monitor*. March 20, 2017. https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar

Segal, A. (2019). The Right Way to Deal With Huawei. *Foreign Affairs*. July 11, 2019. https://www.foreignaffairs.com/articles/china/2019-07-11/right-way-deal-huawei

Segal, A. (2020 A). China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. *The National Bureau of Asian Research.* Special Report no. 87, pp. 85-100. August 2020. https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/

Segal, A. (2020 B). The Coming Tech Cold War With China. *Foreign Affairs*. September 9, 2020. https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china

Shepardson, D. & Freifeld, K. (2019). China's Huawei, 70 affiliates placed on U.S. trade blacklist. *Reuters.* May 16, 2019. https://www.reuters.com/article/uk-usa-china-huaweitech-idUKKCN1SL2VW

The Economist (2019). Huawei has been cut off from American technology. May 25, 2019. https://www.economist.com/business/2019/05/25/huawei-has-been-cut-off-from-american-technology

Trump, D. (2017). Statement by President Trump on the Paris Climate Accord. June 1, 2017. https://it.usembassy.gov/statement-president-trump-paris-climate-accord/

University of Pavia (2019). Nasce il 'Microelectronics Innovation Lab' realizzato in collaborazione tra Huawei e UniPv. July 15, 2019. http://news.unipv.it/?p=41454

van de Sanden, M. & Sickinghe, F. (2020). Act against undesired control in the telecom sector in the Netherlands: new notification requirement and power to block transactions. Kluwer Competition Law Blog, June 11, 2020. http://competitionlawblog.kluwercompetitionlaw.com/2020/06/11/act-against-undesired-control-in-the-telecom-sector-in-the-netherlands-new-notification-requirement-and-power-to-block-transactions/

Van Schaik, L. & Dams, T. (2020). No way back: Why the transatlantic future needs a stronger EU. Clingendael Netherlands Institute of International Relations. November 20, 2020. https://www.clingendael.org/publication/no-way-back-why-transatlantic-future-needs-stronger-eu

von der Leyen, U. (2019). The von der Leyen Commission: for a Union that strives for more. September 10, 2019. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_5542

Xi, J. (2015). Zai di'er jie shijie hulianwang dahui kaimushishang de jianghua (在第二届世界互联网大会开幕式上的讲话) [Speech at the 2nd World Internet Conference Opening Ceremony]. December 16, 2015. http://nl.china-embassy.org/chn/zgyw/t1325883.htm Translation available at: https://chinacopyrightandmedia.wordpress.com/2015/12/16/speech-at-the-2nd-world-internet-conference-opening-ceremony/

Yuan, Y. & Nian, L. (2019). Beijing Orders State Offices to Replace Foreign PCs and Software. *Financial Times*. December 8, 2019. https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406