FACULTAD DE CIENCIAS HUMANAS Y SOCIALES

CHINA AND THE TELECOMMUNICATIONS WAR: THE THREAT OF THE RISING POWER AND ITS IMPACT ON THE INTERNATIONAL ORDER

Autora: Marta Vicioso Benítez
Tutora: Ana Trujillo Dennis
5º E5 (Derecho y Relaciones Internacionales)

Madrid
Mayo, 2020

CONTENTS

1. INTRODUCTION

It is undeniable that China is steadily climbing up the ladder of international politics and is set to become a key player that will determine the geopolitical realities of the future. When the People's Republic of China (PRC) was recognized as the "only legitimate representative of China to the United Nations"[1] in October 1971, the country inaugurated, under the umbrella of the Four Modernizations[2], a period of steady industrialization. This era has allowed China to become the economic powerhouse of the world that today is threatening to quickly overcome the United States as the leader and rule-maker of the global economy. The astonishing rise of China is reflected in the economic data of the last three decades, where the PRC has incremented its gross domestic product (GDP) by 54%, its exports by 143% and its reserves by 3124%[3] (World Bank, 2015). In recent years, these economic achievements have been accompanied by a clear mission to enhance Chinese military power, where the PLA is set to build a Blue Water navy capable of patrolling the oceans and competing with that of the United States.

The potential impact of China's rise on the international order is immediately magnified if we bear in mind the sudden change in the PRC's foreign policy strategy since Xi Jinping's election as president. One of his principle policy objectives is to make amends to the "century of humiliation" that China suffered since the decline of the Qing dynasty in the early 1900s. This misfortune gave way to a period in history that was marked by political and military defeat from the rapidly industrializing imperial powers of the West. For Xi Jinping, this historical past has meant that being the World's Factory is no longer good enough for China, where the country is now prepared to "take center stage in the world and to make a greater contribution to humankind" (Xi, 2017). The 'China Dream' promoted by Xi Jinping aims to resurface China's role as the driver of humanity and modernity, once again converting the country into the Middle Kingdom of Asia. Since 2013, China has therefore shifted its foreign policy strategy from being a mere recipient of globalization, to becoming an architect of global politics. Such refurbishment of the Chinese powerhouse is being achieved by monumental

[1] This decision was adopted by the United Nations General Assembly Resolution 2758, with a vote of 76 for and 35 against.
[2] Deng Xiaoping's Four Modernizations policy aimed to reconstruct five key industries that had been abandoned or unknown to China – agriculture, industry, technology, science and defence.
[3] These economic achievements have been attained with a workforce that is a quarter as productive as that of the U.S. With equal manpower, the Chinese economy would be four times bigger than the American one (Allison, 2017).

infrastructure projects and global strategies such as the *Belt and Road Initiative* and *Made in China 2025*, which intend to transform the country into a key provider of technology and scientific innovation. It is consequently no secret that China is determined to lead the global implementation of Fifth Generation Technologies (5G), which are said to be the key to potential world domination.

The imminent rise of China is threatening to alter the balance of power that has been in place since the end of the Cold War. This is forcing the international order to deal with a state actor whose societal values and strategic intentions are mysterious and hard to understand. The problem is essentially that the international system has never witnessed the *global* rise of a civilization-state, whose society protects the collective over the individual and believes in the value of hierarchy, thus opposing the Western concept of a 'universal civilization'. This means that China will not follow a predictable pattern according to Western understanding, where traditional theories of *Foreign Policy Analysis* (FPA)[4] might prove insufficient to truly comprehend the reasoning and intent behind the decision-making process within the Communist Party of China (CPC). The necessity of understanding China has therefore become more imperative now than ever. Comprehending intention and the culture that determines it is indispensable in order to prevent those irreconcilable differences that could essentially lead to the application of the Thucydides trap[5].

Understanding the key components of China's foreign policy strategy is crucial in order to prevent an abrupt and devastating decline of the current international status quo. In this sense, one of the main drivers of China's global strategy is Beijing's determination to lead the worldwide implementation of Fifth Generation Technologies (5G), through two Chinese technological giants – Huawei and ZTE. The importance given to 5G can be understood in the framework of Xi Jinping's objective to convert China into a global powerhouse in high-tech industries, where 5G technology is consistently mentioned in *Made in China 2025* and the *National Informatization Strategy*. The centre stage of 5G can thus be comprehended if we bear in mind traditional Chinese perceptions

[4] The field of FPA aims to understand the process that has determined a specific decision taken by a state actor and that has directly impacted the international system (Alden & Aran, 2017).
[5] The Thucydides Trap is defined by Graham Allison as the "natural, inevitable discombobulation that occurs when a rising power threatens to displace a ruling power", which is believed to be applicable to U.S. – China relations (Allison, 2017: xvi).

of war and strategy, where the teachings of Sun Tzu[6] determine the clear preference of waging a psychological war, that allows for victory without military intervention. However, although China does not conceal its 5G global programme, the key elements of this strategy are mostly unknown and are yet essential to understand the geopolitical potential of this strategy.

This dissertation therefore aims to analyze the potential of China's 5G global strategy, especially as a means to advance state interests in the South China Sea. To this end, the role of key players will first be presented and analyzed. In this regard, it is no secret that China is leading the global implementation of 5G as a result of the international success of its technological giant – Huawei. Furthermore, the architecture of the 5G network and its inherent security vulnerabilities will be presented, in order to break down its potential as a new and disruptive geopolitical weapon. This technical investigation will allow us to understand how 5G will enable state actors to strike low-profile attacks. The last chapter will be dedicated to analyzing the manner in which Beijing could make use of Huawei's 5G infrastructures along the Digital Silk Road, in order to gain a comparative advantage in the South China Sea. To this end, it will be necessary to research which countries along the Belt and Road Initiative are implementing Huawei 5G technology, and how this could allow China to project its geopolitical interests in the region.

2. STATE OF THE LITERATURE

The question of Fifth Generation of Mobile Technologies (5G) has aroused the interest of academics in the fields of engineering and politics alike, therefore demonstrating its multidisciplinary facet and far-reaching potential impact. The transformative and disruptive new capabilities of 5G have urged information engineers and political scientists to work more diligently now than ever, giving way to rich and extensive literature. However, it is important to understand that these two academic fields

[6] Sun Tzu was a military strategist that around the sixth century BC wrote *The Art of War* – the first study in history to analyze the phenomenon of war from an objective and strategic point of view. His teachings focus on the conception that a victory in war is only truly successful when there has been a preservation both of human lives and of material. Sun Tzu set forth the idea that armed conflict must always be the last resort to achieve strategic goals, only implemented by governments as a means to finish off an enemy that has been previously debilitated and stunned. He therefore established that the function of state spies was absolutely essential in order to collect the necessary information so to silently debilitate the adversary (Cardona, 2017).

analyze both the potential and impact of 5G from different perspectives and on the grounds of different motivations.

Although it is pertinent to present a brief overview of the scientific literature analyzed, the technical limitations and the area of study of this research allow only for a basic outline. In this sense, most of the literature in the field of information engineering explores the use cases and network architecture of 5G from an objective and purely scientific standpoint. For example, a report published by the GSM Association[7] in November 2019 gives a comprehensive insight into the three main service categories that 5G will enable – enhanced mobile broadband (eMBB), Massive Internet of Things (MIoT) and Mission Critical Services (MSC) (GSMA Intelligence, 2019). The report thus analyzes how public and private enterprises can transform and improve their services through the implementation of 5G networks, presenting various MIoT use cases, such as smart cities and smart industrial factories. In addition, a report issued by IHS Markit[8] in November 2019 displays the manner in which 5G technology will enhance those key sectors that are said to be indispensable for the correct functioning of a society, ranging from health to energy (Campbell et al., 2019).

In terms of 5G network architecture, a white paper issued by the FCC Technological Advisory Council[9] explores the manner in which the physical and virtual infrastructures that today support 4G will need to be upgraded or replaced to meet the diversified and highly specialized latency requirements of 5G services (Sparks et al., n.d.). This will be managed through network slicing, a technical term that is consistently mentioned by information engineers. This scientific term refers to the compartmentalization of the network into logical slices that allow for the provision of specific needs to different customers.

Regarding the field of political sciences, the literature that analyzes the geopolitical potential of 5G is broad and extensive. However, due to the extremely volatile nature of a technology such as 5G, where capabilities and conditions are

[7] The GSM Association represents the global interests of mobile network operators around the world and provides an international platform for the resolution of the most pressing issues within the industry.
[8] IHS Markit is a global provider of specialized information for markets and capital-intensive industries.
[9] The Federal Communications Commission (FCC) is an independent agency of the U.S. government that regulates all aspects of communications services.

fluctuating, the search and analysis of this paper's bibliography has been limited to a specific timeline – ranging from 2016 to 2020.

The literature that deals with the geopolitical potential of 5G mainly investigates how this technology can damage critical infrastructures and allow for more discrete and calculated forms of cyberespionage. In this sense, all investigations conclude that the vulnerabilities in both the hardware and software of 5G networks are the main concern. A CCDCOE[10] report issued in 2019 establishes that allowing telecommunications manufacturers access to the core network of a country would provide them with the necessary strategic capabilities to attack those infrastructures that are essential to the security of a state. The virtualization of the core network is also presented as a risk, given that a minor attack in one part could essentially disrupt the entire network (Kaska, Beckvard & Minárik, 2019).

The reorganization of the network for the implementation of 5G services has thus been presented as a potential security threat. A report published by Foreign Policy Analytics illustrates how techniques such as network slicing will essentially increase the attack surface available to those willing to strike an offensive (Perez, 2020). The report also makes reference to the fact that the enhancement of the radio access network (RAN), through the deployment of thousands of new antennas, will create more individualized access points to create 'backdoors' that would be nearly impossible to identify.

One of the consistent dangers mentioned by political science literature is also the fact that a Chinese tech giant, Huawei, is leading the global implementation of 5G networks. A renowned expert in the field of emerging technologies and Chinese military innovation, Elsa B. Kania, established in a November 2019 report that the political and judicial system which Huawei is subject to is a grave concern. This system essentially diminishes the credibility of any statement from the tech giant declaring that it could not be compelled by the Chinese government to advance state interests (Kania, 2019). The author also voices a commonplace concern amongst experts within the field – the reality that domestic efforts will not be enough to free a state from Huawei technology. This is because strategic capabilities of opponents could be hindered in those regions whose infrastructure is predominantly provided by the Chinese tech giant. This connects to the

[10] The NATO Cooperative Cyber Defence Centre of Excellence (CCDOE).

inescapable vulnerabilities of a complex and dependent 5G supply chain, a reality that has been pointed out by James A. Lewis, a political-military expert that has recently centred his efforts on understanding the geopolitics of 5G (Lewis, 2018). The problem is that manufacturing 5G hardware and software components involves dozens of companies with distinct functions in the global supply chain, which means that U.S. telecom manufacturers could never offer an end product completely free of Huawei or ZTE.

Furthermore, the literature analyzing the possible links between Huawei and the Chinese government is thus extensive. A report issued in October 2018 by the Australian Strategic Policy Institute analyzed how the Chinese Ministry of State Security could use accidental vulnerabilities, systematically found in Huawei telecom equipment, to unilaterally introduce backdoors for cyberespionage and cyberattacks. The report sets forth that this strategy could consequently give Huawei space for deniability (Cave et al., 2018). This thesis acquires credibility if we bear in mind the technical security risks found within Huawei devices, which have been studied and reflected in the Finite State Supply Chain Assessment of Huawei Technology[11] (Finite State, n.d.). The report concluded that 55% of all Huawei tested devices had at least one potential backdoor, where the firmware[12] implemented in these devices had significant unsafe and potentially exploitable code conditions. Despite allegations made by Huawei of its efforts to improve these security conditions, the report concludes that analysis of firmware alterations have demonstrated that their defence mechanisms are in fact decreasing.

The possible solutions to be implemented by governments to mitigate the security risks linked to the 5G supply chain and Huawei equipment were also analyzed thoroughly. Experts such as Michael Shoebridge allude to the possibility of establishing institutions such as the Huawei Cyber Security Evaluation Centre (HCSEC), present in the United Kingdom since 2010 (Shoebridge, 2018). In this regard, the HCSEC essentially provides cyber security expertise. Through the publication of annual reports, it analyzes the security status of Huawei telecom equipment present in the UK market and subsequently offers solutions. As Shoebridge points out, the recommendations of the HCSEC have been effective in improving the overall security processes and code quality of Huawei

[11] Finite State is a company that provides insight into the vulnerabilities and risks of the next generation of networks, dominated by the IoT.
[12] Firmware refers to the accompanying software, usually in the form of a microcode inside a processor, that manufacturers of 5G components insert inside their hardware.

equipment. However, the author sets forth that these efforts could only be short-term, due to the lack of control of third-party software implemented in Huawei devices and the source code disparities detected.

In terms of the analysis of how 5G could be implemented by Beijing as a weapon to advance geopolitical interests in the South China Sea, the literature appears to be less abundant and well defined. The main studies regarding this matter mainly analyze 5G as a key component of the Digital Silk Road. In this sense, the investigation carried out by John Hemmings in January of 2020 has provided significant insight into the geopolitical consequences of this new element of the Belt and Road Initiative (Hemmings, 2020). The study is divided into three units that analyze the strategic intent, origins and implications of the Digital Silk Road. The subsequent conclusion that the author displays is that the digital infrastructures implemented throughout Belt and Road countries will give the Chinese government access to large amounts of data that could be used and manipulated to their advantage. Hemmings establishes that the technologies such as 5G and Artificial Intelligence (AI) will essentially enable the Xi Jinping Administration to collect and centralize the necessary data to boost the country's key sectors and consequentially, to export Chinese *savoir-faire*.

Other publications examine the manner in which the Digital Silk Road could give the PLA the tactical capabilities necessary to strengthen its military competitive advantage in the South China Sea. These capabilities are presented as a strategic tool that could enable the Chinese military to nullify the efforts of regional and global competitors. A study published in January 2020 by the Center for a New American Security provides understanding on how China is using 5G big data capabilities to develop new technological structures. In this sense, fibre-optic submarine cables and the BeiDou Navigation Satellite System, are providing the Chinese military with competitive and autonomous capacities in the region, both in peacetime and wartime (Cronin & Neuhard, 2020).

It is therefore evident that the Fifth Generation of Mobile Technologies (5G) has aroused the interest of highly specialized experts in the field of international relations. Multiple authors have contributed to the formulation of an extensive archive of literature that provides a remarkable insight into this disruptive new technology. This reality has therefore allowed for the organisation of a valuable bibliography that will serve as the

foundation of this dissertation. The objective is to synthesize and organize the vast literature found to answer the specific research questions.

However, there were certain aspects regarding 5G and its geopolitical potential that were not found in the literature analyzed. In this sense, although the near totality of the literature examined referenced Huawei as a key player in the geopolitical arena of 5G, its connection with the Chinese government was consistently presumed. This paper therefore intends to analyze how and why the Xi Jinping Administration could compel the tech giant to advance state interests. The market share and power of Huawei was not broken down either, an aspect that proves important when analyzing the influence and scope of a potential non-state actor. Although the literature that examined how 5G could be used as a geopolitical weapon is already extensive, this dissertation aims to break down the core aspects of 5G that transform it into a political target and the specific security sectors that could be attacked. Furthermore, the literature that investigates how 5G could advance Chinese interests in the South China Sea appeared to be more limited. In consequence, this dissertation intends to fill in the gaps found in the literature analyzed, in order to answer the main research question – how Beijing could use 5G to establish a sphere of influence in the South China Sea and become Asia's hegemon.

3. THEORETICAL FRAMEWORK

In order to analyze the rise of China and its impact on the international order, this dissertation will implement the realist approach. This international relations theory is essentially centered on the eternal power struggle between states in their self-interested quest for security. Realism as a theory was first introduced by the prominent ancient Greek historian, Thucydides, who in his narration and commentary of *The Peloponnesian War* analyzed the root causes of international conflict. In this regard, Thucydides set forth the idea that there is no world order maintained by a higher moral justice – world order is anarchic and relations in this system are determined by power. The eternal power struggle between states was illustrated by Thucydides in the famous Melian dialogue[13]: "right, as the world goes, is only in question between equals in power, while the strong

[13] Melos was a small and independent state that found itself in the middle of a power struggle between Sparta and Athens. Although Melos wished to remain neutral in the Peloponnesian War, Athens believed that this island-city was strategically valuable and therefore forced it to take sides in their favour. After all, Melos was seen as a small and weak state that could easily be used as a pawn.

do what they can and the weak suffer what they must" (As cited in Strassler, 1996, p. 352).

There have been two main approaches to the theory of Thucydidean realism – classical realism and structural realism. Although both schools of thought essentially lead to the same aggressive and power-thirsty behavior of states, the root causes of their antagonistic interactions are believed to be different. Structural realists understand that it is the anarchic structure of the international order and the absence of a higher moral guardian that pushes states to pursue power as a zero-sum game. On the other hand, classical realists believe that it is the intrinsic evil nature of human beings – their *animus dominandi* as Hans Morgenthau put it – that leads them to search for power as a means to attain security.

However, it is the structural theory of offensive realism, first introduced by John Mearsheimer in his essay *The Tragedy of Great Power Politics*, that best explains China's geopolitical goals as established by Xi Jinping. Mearsheimer sets forth that the ultimate aim of states is to achieve hegemony, where their quest for security and appetite for power is limitless. This is because states of all shapes and sizes believe that the only manner to ensure one's own security is to become the most dominant country in the system. Mearsheimer therefore believes that status quo powers simply do not exist. On the contrary, defensive realists consider that there is a limit to world power – states fundamentally wish to preserve the balance of power as a means to conserve their security (Synder, 2002). This school of thought, which was developed by Kenneth Waltz in the *Theory of Great Power Politics*, can serve to analyze and understand the consecutive foreign policy strategies implemented by the USSR during the 20th Century. In this sense, after World War II Stalin was centered on establishing satellite states in Eastern Europe, so as to prevent another invasion and to make amends for the geographical disadvantage presented by the North European Plain (Marshall, 2016). The intentions of Stalin were clearly defensive in nature, given that the ultimate goal was to preserve the balance of power in Eastern Europe in order to protect *Mother Russia.* However, the story of Communist China and Xi Jinping is very different. The President of the PRC openly expresses his aspiration to convert China into the Middle Kingdom of Asia, where the hegemonic nature of these geopolitical goals fit best under the theory of offensive realism.

It is important to bear in mind that offensive realists do not believe that world hegemony is attainable, where Mearsheimer presents the notion of the *stopping power of oceans* to demonstrate this. The fundamental idea is that large bodies of water naturally divide powers in the world, a reality that forces states to strive for regional hegemony (Kaplan, 2014). In this regard, the United States is the only country in modern history that has achieved regional supremacy. It is therefore perceived as natural for a rising power like China to emulate this geopolitical strategy in its natural 'side' of the globe – the Eastern Hemisphere. To this end, Beijing understands that the South China Sea will pave the way to hegemony in Asia, just like control of the Greater Caribbean enabled the U.S. to achieve supremacy in the Western Hemisphere. The main difference between the accession to power of the U.S. and China is that, whilst the former implemented tradition military capabilities, the latter is winning the battle in the information realm through digital imperialism.

4. OBJECTIVES AND METHODOLOGY

The main objective of this study is to analyse how Beijing could implement 5G technologies to achieve regional hegemony. In order to answer this specific research question, two hypotheses will be presented and investigated. The first hypothesis to be tested is that the technical innovations of the 5G network make it a powerful geopolitical weapon for state actors with malign intentions. In the light of the foregoing, the second hypothesis would thus be that Huawei, as an essential player in Beijing's 5G strategy, will be coerced by the government to implement its infrastructure in the South China Sea.

This dissertation will therefore implement qualitative research to analyze how 5G technologies will allow Beijing to control the South China Sea, in the absence of a strong and powerful military. Through the collection, analysis and interpretation of previous investigations, the aim is to understand how China could establish a sphere of influence in Asia and deter other powers from interfering in it. In order to present the key components of this research, the dissertation has been divided into three sections.

Firstly, the aim is to present Huawei as the key player in China's telecommunications war, implementing quantitative research to decipher its current market share and its position in the global standardization race. Through the analysis of two important pieces of Chinese legislation, the *National Intelligence Law* and *Made in*

China 2025, the objective is to understand how and why Beijing could compel Huawei to use its information superiority to advance strategic goals in the South China Sea. Secondly, the aim is to lay out the technical vulnerabilities of 5G networks that make it more insecure than previous mobile generations. This technical analysis will consequently serve as the foundation to demonstrate why 5G is the geopolitical weapon of the 21st century, where its ability to destroy critical infrastructure and conduct cyberespionage are presented as the two main reasons. Thirdly, this dissertation presents a case study analysis of the South China Sea – the body of water that could essentially pave the way to regional hegemony. A geopolitical analysis of the South China Sea is first provided in order to better explain why the region is so important to Beijing. The latter part of the case study is centered on analyzing how 5G technologies could be implemented to enhance Beijing's influence and military competitive advantage. The objective is therefore to understand how Huawei's information superiority along the Digital Silk Road could enable Beijing to control the *hearts and minds* of those in the region, consequently legitimizing its sphere of influence. By analyzing how 5G could enhance the PLA's strategic, operational and tactical capabilities in the South China Sea, the aim is thus to demonstrate how Beijing will be able to establish a strong deterrent in the region.

5. ANALYSIS AND DISCUSSION

5.1 HUAWEI AND THE CHINESE GOVERNMENT

5.1.1 Huawei: the Chinese Technological Dragon

Huawei was founded in 1987 by Ren Zhengfei, a Chinese engineer who had previously been Director of the Information Engineering Academy of the People's Liberation Army (PLA). The birth of Huawei coincided with China's reform and opening-up policies introduced by Deng Xiaoping in 1978. This consequently allowed the company to benefit from the newly established Shenzhen Special Economic Zone (SEZ)[14]. Although during its early stages Huawei was a company with regional scope selling basic telecommunications equipment, towards the end of the 1990s it set out to become a multinational telecommunications firm (Chung & Mascitelli, 2015). As of today, Huawei is a major provider of information and communications technology (ICT) infrastructure and smart devices, with presence in 170 countries and a workforce of 194 000 employees worldwide.

In terms of Huawei's position in the 5G supply chain, it is a telecommunications equipment manufacturer. It provides the necessary infrastructure for mobile network operators, such as Telefónica, to provide 5G services to the end-user. Huawei therefore produces the essential hardware and software that allows the wireless network to function, which is composed of the core network[15] and the radio access network (RAN)[16].

Huawei is today the leading provider of 5G telecommunications equipment, essentially as a result of the intense research and development (R&D) investments made by the company since 2010[17]. In this sense, Huawei closed the second quarter of 2019 with 29% of the global telecom equipment market share, well above the performance of

[14] Deng Xiaoping created four Special Economic Zones within China, which were aimed at aiding in the modernization process of the national economy. The financial, investment and trade privileges were to test the viability of the market-oriented reforms introduced within the scope of the Open-Door Policy (Seng, 2010).
[15] The core network is seen as the brain of the wireless network, given that it collects and transports essential data across the RAN structure.
[16] The RAN is the physical telecommunications network, composed of base stations and antenna arrays, that connects end-user wireless devices and data to the core network. The RAN will require the most investment and innovation, given that the low latency and high frequency requirements of 5G services mean that base stations and antennas will need to be deployed closer to each other, as these radio waves only travel very short distances.
[17] In 2018 Huawei invested 15 billion dollars in R&D, which accounts to approximately 14% of the company's global sales revenues (China Daily, 2019).

its competitors Nokia and Ericsson (Perez, 2020). The worldwide presence of Huawei is thus demonstrated by the number of commercial contracts it has secured, which account to 91, many of which have been signed with the governments of developing countries in Asia (Bicheno, 2020). The significance and advantage of Huawei's market position is immediately displayed if we bear in mind that, by 2035, 5G will account to $13.2 trillion of global economic output (IHS Markit, 2019).

The intense participation and contribution of Huawei to the 5G standardization process also reflects its leading role within the competitive landscape. In this sense, standards[18] are essential for the global implementation of 5G services, given that they dictate the equipment and software that will be used for the global development of 5G networks. Telecom technology standards are adopted within the jurisdiction of international regulatory bodies, such as the 3rd Generation Partnership Project (3GPP). The industry standard is chosen by three technical specification groups from among the technology options presented by 5G telecom equipment manufacturers, such as Huawei.

Furthermore, Beijing has greatly influenced the intense standards-setting efforts of Huawei. The IMT-2020 5G Promotion Group[19] was created by the government in 2013 within the framework of a national strategy set to make China the global leader of 5G standards. The technology developed by the Promotion Group is effectively promoted in the 3GPP through an army of engineers and government officials sent and financed by Beijing, where success is in turn encouraged within the core of the 3GPP by Chinese individuals, who hold more than thirty key positions (Duesterberg, 2019). In this regard, Huawei is the most active telecom firm promoting Chinese 5G standards, accounting to 21% of the overall contributions made by Chinese companies, which accounted to 35%. Huawei engineers thus made up 14% of the total meeting attendance within the 3GPP (Perez, 2020). This has allowed Huawei to be the telecom firm with the largest collection

[18] Standards establish minimum performance requirements that must be respected when manufacturing and implementing 5G services, therefore allowing for the interoperability of the global network.
[19] The Promotion Group was established by the Ministry of Industry and Information Technology (MIIT), the National Development and Reform Commission (NDRC), and the Ministry of Science and Technology (MOST), which created an umbrella under which all major Chinese telecommunications organizations and firms could work together to develop innovative and high-quality 5G technology (Perez, 2020).

of 5G declared patents, where 5,855 of its 19,473 5G contributions have been approved by the 3GPP (Iplytics, 2019)[20].

Huawei's portfolio is also an important source of revenue that allows the company to develop more innovative technology to be presented in the 3GPP as standard contributions. This is because the telecom firms whose equipment becomes the industry standard receive royalty payments from companies that need to use that specific technology for the development of their own 5G infrastructure. However, 5G standards and patents are considered to be critical for national security by multiple governments in the West, given that they are a discrete yet powerful tool that can be used by potential malicious actors (Qualcomm, 2017). The problem with patents is that the company who owns it knows every possible detail and potential flaw found within the equipment, therefore possessing the capacity to introduce backdoors for cyberattacks or cyberespionage. Furthermore, China's competitive position in the 5G standardization race allows the equipment of Huawei to be easily commercialized around the world. This is allowing Beijing to build its technological and political influence along the Digital Silk Road, especially since the poorer countries of Asia need the economies of scale that Chinese telecom giants can provide (Kania, 2019).

5.1.2 National Intelligence Law

Huawei consistently denies all allegations that link the company to the Chinese government and the PLA, insisting that it is a private firm that is completely and effectively owned by its employees. The corporate information presented in Huawei's internet page makes reference to the company's independence:

"Through the Union of Huawei Investment & Holding Co., Ltd., we implement an Employee Shareholding Scheme that involves 104,572 employee shareholders. This scheme is limited to employees. No government agency or outside organization holds shares in Huawei"[21].

[20] Chinese firms lead the overall 5G patent race, with a total of 32,166 approved contributions. European firms, such as Nokia and Ericsson, had a total of 30, 718 (Perez, 2020).
[21] This information has been taken from Huawei's website, which can be accessed at: https://www.huawei.com/en/about-huawei/corporate-information

However, Huawei's curriculum of state support and apparent connections to the PLA and the Ministry of State Security significantly outweigh its continuous efforts to deny such accusations. The problem is that Huawei's corporate structure and decision-making processes are not transparent enough to allow these allegations to be denied with solid and unquestionable evidence. An investigation carried out in 2012 by the U.S. House of Representatives Permanent Select Committee on Intelligence[22] concluded that Huawei's contradicting information on its corporate structure, administrative procedures and ownership corroborated the significant influence and control carried out on the company by Beijing (Rogers & Ruppersberger, 2012). The report determines that Huawei is not effectively owned and controlled by employee shareholders, but rather by a handful of senior managers. The company's supposed independence is thus discredited by the recognition made by Huawei, within the framework of the investigation, that Ren Zhengfei is given veto power by the shareholder agreement.

In fact, it is Ren Zhengfei's past as Director of the Information Engineering Academy of the PLA and his current membership of the Communist party that is continuously cited as the main security concern surrounding Huawei. However, the founder of the telecom giant is not the only individual inside the company with past links to the Chinese military. An investigation carried out by the Henry Jackson Society concluded that 25 000 employees were currently working and cooperating with the Chinese Ministry of State Security and the PLA, either directly hired by these government agencies or under a joint project with Huawei (Doffman, 2019). The conclusions of this report acquire solid credibility if we bear in mind that Huawei is the Chinese telecom firm most capable of providing the necessary R&D to materialize Xi Jinping's objective of enhancing the PLA, essentially through the development of 5G military applications. In this regard, Huawei is already believed to be collaborating with the PLA's Information Engineering University (Kania, 2019).

Nevertheless, even if Huawei's allegations of self-determination were sufficiently proved, the legal framework of China could oblige the telecom giant to effectively

[22] The Committee wrote a report analyzing the potential counterintelligence and security threats posed by Huawei and ZTE, after the former requested an investigation on its corporate structure to bring an end to the accusations. In order to examine both telecom firms, the Committee inspected and analyzed open-source and classified information. However, the report sets forth that the security concerns were not sufficiently clarified due to Huawei and ZTE's lack of cooperation and willingness to provide worthy evidence, where the former only contributed unsigned and unauthenticated documents to the investigation.

cooperate with Beijing to advance state interests. The 2014 Counter-Espionage Law and the 2017 National Intelligence Law of the People's Republic of China are the two pieces of legislation that could allow Beijing to compel Huawei to implement its worldwide 5G infrastructure. The problem with these laws is not their apparent ultimate objective, but rather Beijing's interpretation of what national security is and how it should be achieved. The truth is that China's concept of state security does not find a natural boundary at the borders of the PRC but is rather defined within the framework of a broader notion of regional security (Kaska, Beckvard & Minárik, 2019). In this regard, article 7 of the National Intelligence Law establishes that:

"Any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence work known to the public. The State protects individuals and organizations that support, assist and cooperate with national intelligence work"[23].

Similarly, article 22 of the Counter-Espionage Law compels organizations and individuals to provide all the necessary information to allow the intelligence services of China to ensure state security, where refusal is specifically forbidden by the law. It is therefore no secret that Beijing is most likely going to compel Huawei to aid its country in achieving national security in the South China Sea, a region which is openly believed to be China's legitimate backyard.

5.1.3 Made in China 2025

National schemes such as *Made in China 2025* and the *National Informatization Strategy* emphasize the importance of Huawei to the Chinese government. These two strategies aim to convert China into a technological power capable of exporting its innovation and development, mainly within the framework of the global race to implement 5G mobile networks. Achieving technological supremacy is not thought to only boost China's economic prestige but will thus enable Beijing to advance foreign policy goals in the Asia region.

[23] The hierarchical structure of the Chinese society could allow us to comprehend the legitimacy enjoyed by these laws amongst the population, given that Confucianism has taught them "the supremacy of the state over society and of society over the individual" (Allison, 2017, p. 138).

Made in China 2025 aims to enhance and reshape the national industrial sector, consequently converting the country into a technological powerhouse capable of competing with South Korea, Japan and Hong Kong. In this regard, Xi Jinping believes that China is now prepared to outgrow its traditional characterization as the 'factory of the world'. The country is therefore determined to export high-end goods in the near future, where main industries are already making efforts to increase the quality and efficiency of their production chain (Pan, 2019). This 30-year strategy will be developed in three distinct phases, which will be centered on reducing the production gap with other countries, reinforcing China's position as a technological powerhouse, and finally, leading international innovation efforts. In order to achieve these objectives, Beijing is compelling national firms to increase their investment in R&D, improve labour productivity and engage in more sustainable practices, especially in terms of their energy and water consumption (ISDP, 2018).

The *National Informatization Strategy* is specifically centered on the country's cyber performance, aiming to reinforce informatization capabilities amongst the technological sector. In this sense, national efforts to promote R&D, standards and industry development have been centralized, in an attempt to successfully export Chinese 5G technology. Beijing is therefore specifically supporting the efforts of national champions, such as Huawei and ZTE, in a more precise and consolidated manner. Through this national strategy Beijing consequently aims to materialize its foreign policy objective of leading the global implementation of 5G technologies; a goal that can only be truly achieved by Huawei and ZTE.

Furthermore, recent investigation carried out by the *Wall Street Journal* has established that Huawei has received significant funding and subsidies from the Chinese government. The report determines that the tax exemptions, assistance in financing and price reductions granted by Beijing have allowed Huawei to win a competitive advantage of 75.000 million dollars (Yap, 2019). The price reductions of essential technological resources amounted to 30% of the market value, a privilege that would have allowed the tech giant to become the market leader, both domestically and abroad. Although Huawei establishes that the report vehemently manipulates the company's economic data, the mere possibility of such state financing demonstrates how valuable Beijing believes the tech giant to be.

These two national schemes therefore illustrate the strategic importance of 5G to Beijing. For Xi Jinping, this technology is a central and irreplaceable component of a wider foreign policy objective – allowing China to regionally export its economic and political model in a subtle and apparently win-win approach. In this sense, even if the Chinese government does not own Huawei's 5G technologies, it could easily compel the tech giant to provide its data and infrastructure to ensure 'state security'; after all, Beijing drafted the National Intelligence Law and has the power to interpret it to its liking.

5.2 THE INVISIBLE GEOPOLITICAL MIGHT OF 5G

5.2.1 The Technical Vulnerabilities of 5G

In order to comprehend the threat posed by 5G networks to national security, it is first and foremost necessary to understand the technical aspects that make this digital infrastructure more vulnerable to cyber-attacks than previous mobile generations. In this sense, the main problem is that the technical innovations that allow 5G to offer the three new service categories (eMBB, URLLC and mMTC) and that essentially make it the mobile network of the future, are in fact the root cause of its increased vulnerabilities and overall weakness. The architecture of the current telecommunications network will be altered in a manner that will affect both the core network and the Radio Access Network (RAN), where the technical innovations introduced in their respective software and hardware will give rise to differentiated yet equally dangerous security risks.

In terms of the core network, its data routing and transporting functions will be entirely virtualized in the 5G era, therefore becoming a cloud-based software-controlled system. In previous mobile generations, the network core was composed of a hardware-based system, where a central hub containing switches and cables would route the data across the RAN (Perez, 2020). However, the virtualization of this infrastructure for the deployment of 5G services will make the entire network less secure, given that cyber-attacks will become less detectable and therefore less preventable. This is because cyber hygiene capabilities will be significantly reduced, where the insertion of 'hardware choke point's will not be possible. This will consequently deny mobile operators the ability to control the data flowing through the physical infrastructure and detect threats and potential cyber-attacks (Rugge, 2019).

Another innovative feature of the 5G core network is the introduction of network slicing, a technology that will enable mobile operators to offer service-specific networks to clients with disparate and often contradicting connectivity requirements[24] (5GPPP, 2019). This is because network slicing separates the core network into specialized and logical 'slices' that allow for customized connectivity, where each "network slice is an independent end-to-end logical network that runs on a shared physical infrastructure, capable of providing a negotiated service quality" (GSMA, 2017, p.5). However, network slicing is also a menacing technology that creates more attack surface for potential threats, given that the core network becomes greatly decentralized and each 'slice' allows for more surface area that malicious actors can work on. The architecture of the core network will thus become extremely complex, where each network slice will require access to different resources and will consequently need different hardware infrastructure (5G Americas, 2016). In light of the foregoing, every slice becomes a security threat that could give a potential malicious actor access to the entire network, since the artificial intelligence-based software would enable far-reaching capabilities (Perez, 2020).

In terms of the RAN, the innovations introduced to its hardware will also make 5G networks more vulnerable, essentially due to an exponential rise in network access points and reduced detection capabilities of cyber threats. The immense deployment of RAN infrastructure that 5G will require, such as small radio cell towers[25], will grant malicious actors more equipment from which to install backdoors[26] and access the entire network (Rugge, 2019). The number of devices connected to the 5G network will also increase significantly with the Internet of Things (IoT), a reality that will create *even* more end points from which to enter the network. Furthermore, the volume of data flowing through the RAN will rise exponentially as do the billions of connected devices, where it is estimated that 5G networks will carry nearly half of the world's mobile network traffic by 2025 (Jonsson et al., 2019). This will significantly diminish the detection capabilities

[24] It is important to bear in mind that the three service categories enabled by 5G require different latency and frequency capabilities: eMBB services, such as high definition videos, demand high data rates; URLLC services, such as self-driving cars or drone control, require latency-sensitive capabilities; mMTC services, such as smart cities and smart factories, demand extremely high density connection capabilities (Huawei et al., 2017).

[25] The 5G RAN will need to be densely deployed throughout vast geographical areas and will consequently require the most investment. This is because high frequency waves can only travel small distances and are not able to pass through buildings or any other potential obstacle.

[26] A hardware backdoor allows the attacker to bypass the established security mechanisms of a computer system and therefore grants a continued access point into the network.

of mobile operators, who will not be able to manage and control such huge amounts of data (Perez, 2020).

Similarly, the characteristics of Huawei that allow it to be so attractive and competitive as a 5G equipment supplier are in fact what make it a national security concern for many governments. In this sense, Huawei provides the software and hardware infrastructure in both the core network and the RAN, where this innovative end-to-end approach is believed to constitute a grave security risk. This is essentially because providing the equipment of the entire 5G supply chain entitles Huawei to carry out maintenance and service repair activities, consequently giving the Chinese telecom giant continued and justified access to the hardware and software within the 5G network of an entire country. This in turn provides Huawei with the ability to introduce backdoors in the equipment, a reality that has been clearly explained by James A. Lewis:

> "Major telecom "backbone" equipment is usually directly connected to the manufacturer over a dedicated channel, reporting back on equipment status and receiving updates and software patches as needed, usually without the operator's knowledge. Equipment could be sold and installed in perfectly secure conditions, and a month later, the manufacturer could send a software update to gain access to information or to disrupt service. The operator and its customers would have no knowledge of this access and control." (Lewis, 2018, p.9).

The potential security risks associated with the implementation of Huawei 5G equipment are emphasized if we bear in mind the Finite State Supply Chain Assessment of Huawei Technology, which found that 55% of all Huawei tested devices had at least one potential backdoor, where the firmware implemented in these devices had unsafe and potentially exploitable code conditions (Finite State, n.d.). These vulnerabilities were confirmed by the 2019 report published by the Huawei Cyber Security Evaluation Centre (HCSEC) in the UK, which concluded that Huawei thus lacked supervision and control capabilities in terms of third-party software components implemented inside its equipment[27] (HCSEC, 2019).

[27] These third-party suppliers will introduce their own firmware (microcode) in the software components they provide to Huawei. The multiplicity of firmware found in the final product of Huawei means that threats are difficult to isolate and mitigate (Perez, 2020)

5.2.2 The Disruption to Critical Infrastructure

It is important to understand that the threat posed to national security and the geopolitical might of 5G is not determined by the inherent weaknesses of its hardware and software, but rather by the fact that the critical infrastructures of an entire country will be connected to the 5G network and will rely on its technology. The technical vulnerabilities aforementioned simply serve to demonstrate how striking an attack on the fundamental infrastructure of a country could be imperceptible and straightforward, especially for a supplier of 5G infrastructure such as Huawei. In this sense, the problem is that the digital dependency of countries is growing as the Internet of Things (IoT) expands into key industries, such as the Emergency Services Sector (ESS)[28] or the energy industry. This therefore means that the disruption of the 5G network will not just affect individual consumer goods; cyber-attacks now have the potential to shut down an entire country and must therefore become the fundamental national security concern of governments in the 5G era.

The high frequency and low latency capabilities of 5G technologies allow for multiple use cases, which are now encompassing the critical services and infrastructures that allow for the correct socio-economic functioning of a country. It is undeniable that upgrading key industries with 5G technology will improve their overall performance levels, given that their quality of service (QoS), reliability and sustainability will be greatly enhanced (Campbell et al., 2019). For example, the implementation of smart grids to the energy infrastructure of a country could allow for the enhanced monitoring, distribution and management of energy resources; the employment of connected sensor technologies could allow for smart agriculture and therefore improve the overall efficiency of this industry (Ivezic & Ivezic, 2019). The defence sector will also benefit from the implementation of 5G military applications, which will enhance command and control (C2) and intelligence, surveillance and reconnaissance (ISR) capabilities, among others, consequently allowing for the 'intelligentization' of the military (Kania, 2019)[29].

[28] This sector allows for the resilience capabilities of a country and will be of extreme importance in the near future, as natural disasters are increasing due to global warming.

[29] The defence sector will not be able to ensure a supply chain that is free from commercial telecom manufacturers, such as Huawei. They do not have the necessary economies of scale or resources to develop their own 5G military applications. Even if a country, such as the United States, decides to ban Huawei and implement the telecom equipment of Ericsson or Nokia, its defence sector will not be completely free of Chinese 5G technologies. This is because the networks of foreign allies, such as those in the South China Sea, could be built on Huawei 5G infrastructure (Medin & Louie, 2019).

However, the concern is that governments willing to connect critical infrastructure to the 5G network will essentially have to trust their national security to the telecom manufacturers that provide the necessary technology.

It is therefore unquestionable that having the capability to attack the critical infrastructures of a country is a highly disruptive geopolitical weapon that will allow governments to advance strategic interests in a very short period of time[30]. This means that 5G security has to become the national priority of governments around the world. However, the underlying problem may not be national political willingness or international cooperation in cybersecurity, but rather the inherent technological vulnerabilities of 5G that prevent it from being strengthened and secured. In this sense, whilst it is true that 5G will open a world of new possibilities, the increased insecurity of this new technology may well constitute the inevitable and insuperable collateral damage of its worldwide deployment.

5.2.3 Data Trafficking and Cyberespionage

The international deployment of Chinese 5G technology could also allow Beijing to enhance the intelligence collection activities of the Ministry of State Security and the People's Liberation Army (PLA). The 5G infrastructure of Huawei deployed in the core network of a country could constitute a powerful signals intelligence (SIGINT) collection method at the service of the Chinese government. In this sense, signals intelligence allows for the collection and exploitation of electronic communications between systems, such as computers; devices that will be connected to the 5G network. The problem is essentially that the complexity of this new network will allow Beijing to introduce imperceptible 'backdoors' in Huawei's infrastructure, continuously feeding the country's intelligence service with updated data. Moreover, these 'backdoors' might take *years* to be detected and removed, therefore allowing the Ministry of State Security and the PLA to collect political and economic intelligence for long periods of time. In this way, it

[30] Although critical infrastructures have been subject to cyber-attacks in the past, the cyberweapons implemented by governments were much slower to develop. For example, the Stuxnet worm that paralyzed Iran's nuclear program took years to bring into existence – although it was discovered in 2010 it is thought to have been in development since 2005 (and was therefore carried out under 3G technology). The success of this cyberweapon thus depended on a human error. The Stuxnet worm had to be involuntarily introduced into the Natanz nuclear facility by an Iranian worker through a USB drive, given that the nuclear plants were not connected to the internet. This therefore demonstrates that 5G will allow for quick and direct cyber-attacks, not only due to the increased potency of the mobile network itself, but because critical infrastructures will already be connected to the internet.

provides the Chinese government with valuable information from which to shape, to its own advantage, its foreign policy and diplomatic moves (Johnson & Wirtz, 2011).

Huawei's ability to use its infrastructure in order to carry out cyber espionage was revealed after *Le Monde* published, in January 2018, an investigation disclosing a cybersecurity scandal in the Headquarters of the African Union. The report established that the building in Addis Ababa, which was built and financed by the Chinese government, sent data to an unknown server in Shanghai for two hours every night (Cave et al., 2018). Huawei had signed a telecom contract with the African Union Commission in 2012, which enabled the Chinese company to install the Wi-Fi, storage sharing and computing system of the entire building (Shoebridge, 2018). This cybersecurity scandal, which has been corroborated by multiple newspapers and international think tanks, could somehow foreshadow an intelligence partnership between Beijing and Huawei. Taking into consideration the lack of a technological competitors in the African continent, the data collected in the Headquarters of the AU could not have served any corporate interest of the Chinese telecom giant. The main hypothesis is thus that the data was collected to serve broader political goals established by Beijing.

Furthermore, in a world in which the Digital Revolution is making societies and individuals more dependent on the internet by the day, not only is Beijing becoming increasingly powerful due to the amount of information it is able to gather, but it is also being able to carry out its endeavors without restraint. Operating within a domain that is yet to be regulated internationally, 5G technology allows for the cyber-espionage that existing regulations impede the military from undertaking. The lack of international standards of conduct therefore allows for plausible deniability and the power to deflect accountability (Kissinger, 2014). As Kerry Brown sets forth:

> "In cyberspace, there is a golden opportunity to put up a fight in a place where there are no agreed international conventions and where confusion and obfuscation can reign. It is the only true frontier territory left, and one that China feels it has every right to try and to colonize" (Brown, 2017, p.98).

5.3 CASE STUDY: THE SOUTH CHINA SEA

5.3.1 The South China Sea: China's Backyard

"It is a harsh but true reality: capitalist prosperity leads to military acquisitions. States in the course of rapid development do more trade with the outside world, and consequently develop global interests that require protection by means of hard power" (Kaplan, 2014, p.32).

This perfectly depicts the development phase in which China finds itself today, where the consolidation of its economic and political power will greatly depend on the PRC's ability to exert hard influence in regional hot spots, such as the South China Sea. As Robert D. Kaplan sets forth, China is merely following in the footsteps of the United States' strategy in the Greater Caribbean, where the Monroe doctrine of 1823 was the opening gambit in the wider geopolitical aim of becoming the exclusive superpower of the region[31] (Kaplan, 2014). In this regard, China's unconcealed strategic goal of controlling and securing the South China Sea, which it regards as its rightful backyard, appears to fall within the natural course of action of a rising superpower that is beginning to look outward into the wider world.

The geopolitical value of the South China Sea stems from the fact that it is possibly the world's most important regional waterway. Harbouring the annual transport of 30% of international commerce, which amounts to approximately 5.3 trillion dollars' worth of goods, it is justly believed to be the world's maritime artery of trade (CSIS, 2016). The natural resources found within the seabed of the South China Sea thus highlight its strategic potential, where recent explorations of the ocean floor show that it harbours 11 billion barrels of oil and 190 trillion cubic feet of natural gas (CSIS, 2018). Spanning an area of 3.5 million square km, the South China Sea possesses one of the largest and most diverse marine fisheries in the world, a reality that converts it into a massive provider of protein-based foods for the surrounding countries in the region (Sumalia et al., 2019)[32].

[31] The importance of the Greater Caribbean to the United States was clearly depicted during the Cold War. It became clear that Washington would not allow Cuba to become another pawn in the USSR's influence campaign, even risking the outbreak of a nuclear war following the Bay of Pigs Invasion in 1961.

[32] Marine fisheries acquire importance if we bear in mind that a fish-based diet is a cheap and nutritious solution for countries within the South China Sea that need to feed massive populations. Securing this

It is therefore no secret that controlling trade, docking, patrol and military rights in the South China Sea would open a world of geopolitical possibilities, which means that everybody wants a slice of the cake. For about half a century, the Philippines, Vietnam, Malaysia, Brunei, Taiwan and China have been making territorial claims to 200 tiny islands and reefs, as well as their surrounding waters. These are mainly found in the heart of the disputed region. However, China makes the most ambitious claim, affirming that on historical grounds the near totality of the South China Sea is under its exclusive sovereignty. The CPC argues that the disputed lands were discovered and conquered by Chinese expeditions carried out since the beginning of the second century BC, a reality that consequently delegitimizes any subsequent claim made by a state (Malik, 2013).

The truth is that China has more at stake in the South China Sea than any other opponent in the region. The rules of geopolitics dictate that superpowers must secure the major logistics routes that their industries depend on, especially in preparation for wartime. As the world's leading consumer of imported energy and raw materials, China's future resource security will depend on its ability to prevent the maritime routes in the South China Sea from being blocked during conflict. In this sense, one of the major geopolitical vulnerabilities of China in the region is its dependence on the Straits of Malacca[33], a strategic chokepoint through which 80% of the country's imported oil must pass (Singh, 2019). This unfavorable scenario was denominated by Hu Jintao as the 'Malacca Dilemma'[34], a term that continues to apply to an overdependent China that will need to find new solutions in the South China Sea to secure its increasing oil imports.

Apart from these geographical hindrances, control of the South China Sea also serves one of Xi Jinping's central foreign policy objectives, which is to dust off China's self-consideration as the Middle Kingdom of Asia. This notion of China's global role is based upon the foundations of the 'ancient civilization', where the foreign relations of the different Chinese dynasties were based on a hierarchical system in which all peripheral countries served as natural tributaries (Allison, 2017). As China is waking up from the

natural resource is strategically important today, as global stocks of fish are dramatically falling (Martin, n.d.).

[33] The Strait of Malacca is a narrow stretch of water that passes through Malaysia, Indonesia and Singapore; three countries that are diplomatically allied with the United States.

[34] One of the strategic objectives of the Belt and Road Initiative (BRI) is to reduce the 'Malacca Dilemma', where China is building pipelines and canals to find alternative land routes for the transportation of energy resources to the Chinese mainland.

century of humiliation, it is determined to take up its lawful position as regional hegemon. This role had, in the eyes of Beijing, been temporarily assumed by the United States since the end of the Second World War. From a legal and economic perspective, control of the South China Sea will therefore allow Beijing to consolidate its role as natural hegemon, where the region could very well be a mirror of future global power relations and dilemmas, with China taking centerstage.

In order to achieve its strategic goals in the South China Sea, the PRC is challenging classical interpretations and understandings of maritime legal rights. On the basis of the nine-dash line, Beijing establishes that "China has indisputable sovereignty over the islands in the South China Sea and the adjacent waters, and enjoys sovereign rights and jurisdiction over the relevant waters as well as the seabed and subsoil thereof" (Permanent Mission of the PRC to the UN, May 2009). Although the ambiguity of such statement allows for multiple interpretations, it seems clear that Beijing has provided itself with extensive territorial and exclusive economic zones within the South China Sea[35], by claiming those that sprout from the lands and physical features within the nine-dash line. This distorted interpretation of international treaties, such as the United Nations Convention on the Law of the Sea (UNCLOS)[36], has allowed China to rewrite the legal framework of the South China Sea in a manner that allows it to advance strategic interests, essentially on the grounds of an artificially created legitimacy. Such presumed legal founding has already allowed China to unilaterally dredge and reclaim seven sites in the Spratly Islands, such as Fiery Cross Reef, which are significantly extending Beijing's military strategic capabilities and effective control of the region.

However, China understands that controlling the South China Sea will not be possible without a Blue Water navy, an indispensable asset that Beijing is determined to acquire. This ambition is being fulfilled through the Chinese aircraft carrier program, which is set to not only extend the country's naval capabilities, but also significantly boost its national prestige. On the 17th December 2019, the first Chinese-built aircraft carrier, the Shandong, was brought into effective working condition, where a third is under construction and will be commissioned in 2021. China is thus committed to expanding

[35] Chinese claims of territorial sea and exclusive economic zones within the South China Sea directly contravene articles 3 and 57 of UNCLOS, which establish that the breadth of these domains must not exceed 12 and 200 nautical miles respectively. Chinese claims run as far 2000km from their mainland.
[36] China also challenges the definition of Freedom of Navigation universally accepted, which includes military operations (Congressional Research Service, 2020).

the crown jewel of the navy – the submarine fleet. This part of the Chinese armada is composed of imperceptible and dangerous machines that are increasing the PLA's offensive capabilities in the region (Allison, 2014). Notwithstanding, Beijing's maritime defence strategy will not only allow China to achieve wider foreign policy objectives in the South China Sea but could also define and alter the future world order. As geopolitical expert Tim Marshall points out:

> "In the medium to short term, as it builds, and trains, and learns, the Chinese navy will bump up against its rivals on the seas; and how those bumps are managed – especially the Sino-American ones – will define great power politics in this century" (Marshall, 2016, p.50).

5.3.2 The Digital Silk Road

It is unquestionable that the South China Sea is a strategically important hotspot for Beijing. However, Xi Jinping understands that the PLA is not yet prepared to carry out the geopolitical objectives aforementioned. Using traditional military power, as Washington did with the U.S. navy in the Greater Caribbean, is not an option. China is therefore using the economic and technological resources at its disposal in order to pursue strategic objectives in the region. Since 2013, Beijing has centered the near totality of these assets to develop the largest investment and infrastructure project in human history – the *One Belt, One Road* Initiative (OBOR). The astronomical dimension of the OBOR is clearly demonstrated by the figures that outline is worldwide scope – it covers 60 countries, 55% of the world's GDP, 70% of the world's population and 75% of its energy resources (Hemmings, 2020). The economic aim of the OBOR is to bring connectivity to Eurasia and the countries bordering the Indian Ocean, in terms of resources, goods and technology (Allison,2017). Nevertheless, the underlying geopolitical objective is to allow China to lead a 'pivot to Asia', where the rules of the game are effectively determined and controlled by Beijing.

The technological component of the OBOR, the *Digital Silk Road*, has been taking centerstage in terms of the South China Sea struggle since 2015. The aim of the Digital Silk Road is to bring internet connectivity around the Southeast Asia region and Europe (Shen, 2018). For the materialization of this technological objective, Beijing is essentially enabling Huawei to establish the 5G infrastructure within those countries participating in

the OBOR. However, Huawei is not just installing the cellular network for the deployment of 5G technology, it is also exporting its *smart city* and *smart port* models (which combine 5G services and Artificial Intelligence). The main concern is therefore that Beijing will have access to huge amounts of valuable information, which the Chinese Intelligence Services and the PLA can use for malign purposes. The Digital Silk Road is thus enabling China to successfully export its *modus vivendi* – its political system, its technological companies and its international standards (Bartholomew, 2020).

In order to comprehend the potential of the Digital Silk Road and Huawei in advancing geopolitical objectives in the South China Sea, it is first important to lay out their expansion and scope in the region. In this regard, Thailand, Cambodia, Malaysia and the Philippines are four states that to this day have publicly announced 5G contracts with Huawei (Perez, 2020). Furthermore, Brunei, Thailand, Hong Kong, Myanmar, Singapore, Indonesia and Vietnam are all participating countries in the OBOR (OECD, 2018). This means that directly through Huawei, or indirectly through the Digital Silk Road, Beijing can exert some form of technological control over all those states with which China has competing interests in the region. It is therefore essential to analyze and understand how Beijing could use the information collected through 5G infrastructures to establish an undisputed sphere of influence in the South China Sea.

5.3.3 The Sphere of Influence in the Digital Age

"Power is in tearing human minds to pieces and putting them together again in new shapes of your own choosing" (Orwell, 1949).

In his dystopian novel, *Nineteen Eighty-four*, George Orwell depicts the horrors of a totalitarian state whose propaganda, surveillance and censorship capabilities completely nullify citizens as human beings, who are not even free in their own minds. Although during the 20th Century the technological powers of *Ingsoc*[37] appeared to be limited to the fictional world of Orwell's novel, 5G and Artificial Intelligence (AI) today allow for the materialization of the nightmarish state illustrated in *Nineteen Eighty-four.* In this regard, through the Digital Silk Road and its key component, 5G infrastructures,

[37] The *English Socialist Party (Ingsoc)* is the fictional political party that governs the totalitarian state in George Orwell's novel.

China may well be on its way to establishing a Big Brother society in the South China Sea. The implementation of Big Data capabilities will enable Beijing to shape the hearts and minds of the entire region in a manner that satisfies its strategic interests. The continuous psychological manipulation and physical control of individuals will therefore allow China to install an effective and undisputed political, economic and cultural sphere of influence in the South China Sea.

By controlling and manipulating the data flowing through 5G infrastructures in the region, Beijing is enhancing its 'discourse power'. In this sense, the projection of discourse power enables the Chinese government to control information and ideas in a manner that advances its foreign policy objectives, through the promotion of certain perceptions or narratives and the suppression of others (Riikonen, 2019). Discourse power essentially aims to control the mindset of adversaries in order to prevent them from taking decisions that could potentially harm Beijing's interests, therefore cultivating a strategically favorable environment to China both in peacetime and wartime (Kania, 2016). In consequence, discourse power is an evident materialization of one of Sun Tzu's principle teachings – "to fight and conquer in all our battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting" (Cardona, 2009, p.32). Chinese strategists believe that controlling the psychology of an enemy through the careful manipulation of information and the media is much more valuable than a victory on the battlefield, given that it allows the PLA to acquire momentum in the strategic terrain in a manner that deters adversaries from attacking (Allison, 2017).

Discourse power has been a fundamental part of the PLA's military strategy since 2003, when the concept of the 'Three Warfares' was first introduced in the *Political Work Guidelines of the People's Liberation Army.* In this regard, the 'Three Warfares' can be defined as:

> "A unique Chinese political warfare model that calls for the coordinated use of psychological warfare, public opinion warfare, and legal warfare to establish 'discursive power' over an adversary – that is, the power to control perceptions and shape narratives that advance Chinese interests and undermine those of an opponent" (Costello & McReynolds, 2018, p. 28).

The 'Three Warfares' therefore encompass three different kinds of information operations to be implemented by the PLA during peacetime and wartime. The main objective is to delegitimize the strategic intentions of an adversary and promote internal divisions within that country, so to disrupt its will to fight or interfere with China's foreign policy objectives (Kania, 2016). However, it is important to bear in mind that Beijing's information campaign is *not* an element of China's soft power projection[38]. The dissemination of manipulated information and the censorship of specific narratives and opinions clearly respond to hostile intentions. In consequence, discourse power should be regarded as a kind of sharp power with Chinese characteristics; in other words, the projection of hard power in the information realm.

Although discourse power has been implemented by the PLA for nearly two decades, 5G is set to significantly enhance its information capabilities and therefore allow Beijing to slowly but steadily advance its objectives in the South China Sea. This is because the Ministry of State Security can now introduce backdoors in Huawei's 5G infrastructure deployed in countries within the region, in order to grant the Chinese intelligence services with access to high volumes of valuable information. In this regard, Artificial Intelligence (AI) has thus diminished the limitations related to the treatment and management of big data, where an AI application known as machine learning is developing the ability of computers to process, filter and analyze all the data collected from devices connected to the 5G network (Riikonen, 2019). This means that Beijing will have access to highly specialized personal and industrial information, which will allow it to tailor micro-targeted propaganda and disinformation campaigns[39]; a reality that in turn will enable the Chinese government to successfully extend its discourse power in the

[38] An element of Beijing's soft power strategy, for example, is the movement of people in and out of China since 1978. Chinese tourists are seen by Beijing as a valuable tool to export the country's history, language and culture, therefore overshadowing the negative impressions of the CCP that are typically held by individuals in the West (Brown, 2017).

[39] The power of using personal data for political purposes was clearly demonstrated after the Cambridge Analytica scandal was uncovered in 2018. This political consultancy firm, which was hired by Trump's 2016 presidential campaign, used the digital footprint of over 50 million Facebook users in order to create distinct psychological profiles. This in turn allowed them to tailor specific Facebook ads promoting those aspects of Trump's political program that fitted best with the needs and fears of the different profiles. The most alarming aspect of this scandal was the fact that Cambridge Analytica managed to decipher an individual's personal attributes with a few Facebook likes, which demonstrates how technology now has the potential to grant governments the ability to understand the psyche of an individual to control them more effectively.

South China Sea. The implementation of these 5G technologies of disruption will therefore grant Beijing the necessary tools to implant a Big Brother society in the region, through psychological manipulation and physical control.

In this regard, China is first determined to win the war of ideas through the promotion of Xi Jinping's 'China Dream'. This slogan, which began circulating in 2013, refers to the idea that China is finally prepared to reconstruct its natural position at the forefront of modernity, establishing itself as the new Middle Kingdom of Asia (Brown, 2017). The Middle Kingdom refers to the period in history when China was considered the cradle of humanity and the only entity that lay between heaven and earth, where all neighboring states were mere subjects at the service of Beijing (Allison, 2017). The 'China Dream' is therefore Xi Jinping's strategy to enhance the sentiment of national pride amongst Chinese civilians, whilst also cultivating a sense of admiration towards the Middle Kingdom from states within the South China Sea. However, through the 'China Dream' Beijing is thus determined to promote a clear alternative to the socio-political model promoted by the West, which the CCP claims does not represent the ancestral cultural values shared by *all* countries in the region[40] and that were first introduced by the Middle Kingdom. It is therefore apparent that Beijing aims to brainwash individuals with an emotional message that creates an 'us v. them' sentiment, where the West is depicted as an outsider that has never rightfully represented the Confucius values of Asian societies. In consequence, intense propaganda and disinformation campaigns could allow the CCP to win the *hearts* of those in the South China Sea, allowing it to create a highly effective moral and political sphere of influence.

Beijing is also amplifying its physical control capabilities in the South China Sea through the establishment of a regional surveillance architecture along the Digital Silk Road. The exportation of Huawei's *smart city* model is essentially allowing the Chinese government to implement and promote its digital repression system in countries within the region. A smart city combines 5G infrastructure and Artificial Intelligence (AI) to infuse technology into every aspect of a city's operations, from its public transport to the

[40] China promotes the notion of the civilization-state to compete with the nation-state, a political organization that was adopted by most Western countries after the Treaty of Westphalia. Beijing believes that the nation-state does not represent the ancestral values of most Confucian societies in Asia, which value hierarchy and the supremacy of the collective over the individual.

underground water system (Hemmings, 2020). However, it is the security component of Huawei's smart city that will enable Beijing to export its digital authoritarianism[41], which will serve to effectively suppress the opposition and control the rise of potential dissidents. These *safe cities* combine different AI biometric recognition methods, such as high-resolution cameras and facial recognition, in order to detect physical signs of disloyalty and exert citizen control[42]. These forms of physical surveillance can thus be complemented with enhanced systems of digital censorship within the South China Sea[43], where the PLA will be able to block content that is hostile to Beijing and even prevent unsympathetic political candidates from being elected (Kendall-Taylor et al., 2020). The overall combination of physical control, censorship and election interference will enable Beijing to, in time, control the *minds* of citizens within the South China Sea and establish a powerful political sphere of influence.

The Chinese cultural and political sphere of influence could be secured even further with the creation of a clear enemy – the West. It is no geopolitical secret that the illustration of a menacing rival has for centuries allowed societies to reinforce their internal sense of unity, where the securitization of an external target is thus an effective strategy implemented by leaders willing to distract civilians from domestic problems and fragilities (Baños, 2019). In this regard, China could create micro-targeted disinformation campaigns, enhanced with the use of deepfake technology[44] to simulate Western politicians threatening with attacking countries in the South China Sea, for example, in order to present Beijing as the natural and legitimate guardian of the region. By presenting the West as a menacing outsider that is determined to undermine the collective values of the 'South China Sea society' (where the idea of the regions cultural and historical universality will be continuously promulgated), Beijing will be able to

[41] Huawei has already exported its safe city model to over a dozen authoritarian regimes, mainly in Africa. For example, the Ugandan government has implemented Huawei's digital surveillance technology to hack the social media accounts and electronic communication of politicians unsympathetic towards the regime (Kendall-Taylor et al, 2020).

[42] The *safe city* model is already being implemented by Beijing in the Xinjiang region to repress the Uighur population. This minority Muslim group is effectively controlled by surveillance cameras deployed in the cities within the region, where AI facial recognition determines which individuals pose a 'security threat' and those that do not.

[43] Digital censorship is today essential for authoritarian governments, given that social media has already proved to be an effective tool to organize mass protests and uprisings, as occurred during the Arab Spring in 2011.

[44] Deepfake technology, which is made possible by AI, allows the manipulator to use an unrealistic audio or visual media to simulate a politician making a public statement (Riikonen, 2019).

validate many political actions in the name of the common well-being and safeguard of the region.

It is important to bear in mind that China's overall discourse power is being projected at a moment in history when the credibility of the United States and Europe is in steady decline, essentially due to the distorted use of Twitter by Donald Trump and the ever-present fragmentation of the EU. This will consequently allow China to, in time, win the psychological war in the South China Sea. The offensive strategies implemented by Beijing in the information realm are allowing it to legitimize its political, economic and cultural sphere of influence in what it regards as its natural backyard. The cultivation of an 'us v. them' mentality may well mean that any future interference from the West in the South China Sea could be seen as an intrusion, where Beijing is successfully relocating the United States and its allies back to their natural 'side' of the earth and implementing 5G capabilities to make it seem as an emotional appeal from the regional civilians themselves.

5.3.4 5G and the PLA: China's Competitive Advantage

Although Beijing's strategy in terms of psychological manipulation and physical control of individuals is greatly offensive, it understands that the PLA does not yet have the military power to directly challenge the United Sates in combat. The Chinese government is therefore consolidating the PLA's defensive capabilities in the South China Sea, in order to create a competitive and strategic playing field that is entirely favorable to China. This will serve to create a powerful deterrent in the region, where the overall combination of offensive and defensive strategies will enable Beijing to further consolidate its sphere of influence and consequently establish itself as the regional hegemon of Asia. Nevertheless, the information provided to the Chinese government by 5G technologies will be equally important, given that it will allow the PLA to significantly enhance its military intelligence and develop denial and deception capabilities.

The reality is that the Digital Silk Road, especially that which runs along the South China Sea countries, could soon become one of the largest intelligence-collection networks the world has ever seen (Hemmings, 2020). This will bless the PLA with strategic information superiority in the region, that in turn will enable Beijing to take

timely and preemptive political and operational decisions. In this regard, it is important to bear in mind that whilst 5G will enhance the PLA's intelligence collection capabilities, AI will also provide the necessary technology to decipher an opponent's encrypted communication channels and will therefore accelerate the process of intelligence analysis (Segal, 2018). This means that 5G and AI will prevent China from being subject to a surprise attack in the South China Sea, given that a military intelligence failure will be highly improbable[45]. The PLA's strategic supremacy will also be enhanced through improved denial and deception capabilities, which will essentially deny an opponent the indispensable information to develop a well-timed and accurate estimate of what is happening[46] (Johnson & Wirtz, 2011). This is because denial can enable the PLA to conceal its objectives or its capabilities and weaknesses, whilst deception can serve to create a second misleading reality that manipulates an enemy's expectations and offers them an inaccurate sense of intentions and capabilities. The overall strategic advantage in the South China Sea will enable Beijing to always seize and maintain the initiative on the battlefield.

Furthermore, 5G and AI are also set to significantly enhance the PLA's tactical and operational advantage in the South China Sea. Beijing is already implementing these emerging technologies to transform the PLA into a highly intelligent military force that is able to combine its information and technological superiority to strike quick and effective attacks. In this regard, the PLA is developing 5G military applications to enhance its C4ISR capabilities (command, control, communications, computers, intelligence, surveillance and reconnaissance). These organizational and technological capabilities have already been implemented in the Spratly Islands and are proving to be effective in the intelligence collection of maritime conditions and traffic in the South China Sea, therefore granting the PLA with enhanced situational awareness (Cronin & Neuhard, 2020). The tactical and operational capabilities of China's military force are

[45] The importance of high-quality military intelligence was clearly demonstrated after the attack on Pearl Harbor in December 1941, which came to be known as the biggest intelligence failure in U.S. history. The main problem was that a serious miscalculation of Japan's intentions and capabilities failed to provide a timely distribution of relevant strategic information to policymakers.

[46] The deceiver needs to develop and consolidate high quality intelligence about the opponent for denial and deception to be successful. Only then can the misleading information be provided without raising suspicion and whose content is credible enough to trick the target. An example of a highly successful denial and deception operation was when the Allied Forces fooled the Germans into believing that D-Day landings would take place in Pas de Calais rather than in Normandy, a deceit that essentially gave the Allied Forces the necessary strategic advantage to win the war in Europe .

also being improved through the regional expansion of China's own satellite navigation system, BeiDou[47], which will allow the PLA to reduce its reliance on GPS, the satellite navigation system of the United States (Cheney, 2019).

The 5G infrastructure of Huawei deployed in countries within the South China Sea can also be used by Beijing as a pawn to enhance the PLA's competitive advantage in a potential conflict. The possibility of shutting down the critical infrastructure of an opponent and consequently denying it access to basic services could determine a Chinese victory in the battlefield almost immediately. In this sense, one of Huawei's 5G critical infrastructure models, the *smart port*, could prove to be especially valuable to Beijing during a conflict. The smart solutions offered by Huawei essentially digitalize the key functions of a port in order to improve productivity levels in the unloading of containers and ship traffic, therefore reducing logistics costs (Ship Technology, 2018). However, the ability of Beijing to shut down key ports in the South China Sea, preventing containers from being removed and delaying world trade, could enable the Chinese government to exert uncontested global economic pressure and therefore distract opponents from the battlefield (Hemmings, 2020).

The overall combination of China's offensive strategies in the information realm and defensive capabilities in the military playing field are allowing Beijing to establish a powerful deterrent in the South China Sea. This reality is essentially empowering China to extend its main geopolitical goal in the 21st Century – to become the undisputed regional hegemon and revive its rightful place as the Middle Kingdom of Asia. Beijing's successful psychological war is steadily legitimizing its sphere of influence in the region, where winning the hearts and minds of those in the South China Sea could may well mean that all Asian states (whether small or large) will eventually fall like dominoes to China's compelling digital imperialism.

The ability of the United States to counteract the effects of China's psychological war and undermine its sphere of influence in Asia are seriously hindered in a post-Cold War world, where foreign policies such as containment (which was supported by the

[47] Another key component of the Digital Silk Road, quantum computing, has allowed China to set the stage for the development of a quantum compass, which could be used by the PLA's naval vessels for maritime orientation in case the BeiDou system is undermined by an opponent during conflict (Cheney, 2019).

domino theory) could not be implemented today without appearing to be hegemonic in nature (Kaplan, 2014). Furthermore, the United States will find it equally challenging to arouse public support for a war in the South China Sea, given that, despite Trump's numerous attempts to demonize China, the intense securitization of the Middle East during the Bush Administration continues to absorb the attention of the majority of the U.S. population. The strategic, operational and tactical superiority of the PLA in the South China Sea also means that the United States could risk fighting a long and draining war with China, a reality that obliges Washington to think twice before engaging the Seventh Fleet in a war that would be fought very far away from the U.S. mainland.

China has therefore successfully implemented its technological capabilities to forge an effective political and military deterrent in the South China Sea, whose collateral effect is the consolidation of Beijing's sphere of influence in the region. The information superiority made possible by Huawei's 5G technology is essentially allowing Beijing to steadily delegitimize the 'pivot to Asia' promulgated by the Obama Administration in 2009 and continued by President Trump. This allows us to conclude that in a 5G era, which is unquestionably being dominated by China, U.S. supremacy in the Western Pacific is slowly coming to an end. The 5G network in the South China Sea is therefore paving the way for the region's previously dormant superpower to take up its legitimate seat as the natural hegemon of Asia.

6. CONCLUSION

This dissertation has analyzed how the Chinese government could make use of Huawei's 5G technology to create a sphere of influence in the South China Sea. In order to do so, this study has drawn on the offensive realist approach. This theory has allowed us to understand Beijing's broader intentions in the region, where it has been concluded that 5G will be implemented to make amends for the absence of a strong military. For the purpose of answering the research question, the possible association between Beijing and Huawei was first analyzed. Secondly, the technical vulnerabilities of 5G as a mobile network were investigated, to better understand how it could be used as a weapon to attack critical infrastructure and conduct cyberespionage. Thirdly, the study has examined how 5G information superiority and military applications could be implemented to advance geopolitical goals in the South China Sea.

It has been found that Huawei could be compelled by the Chinese government to advance strategic interests in the South China Sea, essentially due to the political and judicial system which the tech giant is bound to. Although Beijing denies that it could use Huawei's 5G infrastructure for malign purposes, the *National Intelligence Law* legitimizes such conduct in the name of the PRC's 'national security'; a notion that is interpreted by the Chinese government to its liking. In terms of the vulnerabilities of 5G, the innovations made to the software and hardware of its network have proved to be the main problem. The virtualization and complexity of the network has meant that introducing 'backdoors' could be straightforward and imperceptible. This allows for enhanced cyberespionage capabilities and the ability to strike a quick attack on the critical infrastructures of a country, given that such systems will be connected to the internet. Furthermore, the capacity to conduct cyberespionage and attack critical infrastructures are two tools that are allowing Beijing to establish a sphere of influence in the South China Sea. Through the intense collection of valuable personal and commercial information, China is successfully launching tailored propaganda and disinformation campaigns to win the hearts and minds of individuals in the region. Furthermore, the PLA is implementing 5G technologies to enhance its strategic, operational and tactical capabilities in the South China Sea (further developed by the possibility of attacking critical infrastructures). These military capabilities are creating a powerful deterrent in the region and are consequently securing Beijing's sphere of influence from a military attack.

China is therefore using the instruments at its disposal – economic and technological supremacy – to successfully advance geopolitical goals in the South China Sea. Through the combination of 5G technologies and Sun Tzu's teachings of "breaking the enemy's resistance without fighting", Beijing is demonstrating that military might is no longer indispensable to achieve regional hegemony. This demonstrates that great power politics are now being carried out in the information realm; a domain in which China has secured a leading position. Information security must therefore become the priority of governments in the 5G era, given that national security is today more at stake than never before. However, the intrinsic vulnerabilities of 5G as a mobile network could essentially hinder the endeavors carried out by governments to secure their country's critical infrastructure and networks. In consequence, it is indispensable for future studies to investigate innovative and far-reaching solutions to secure 5G infrastructures from malign intentions.

Huawei's 5G technology and China's subsequent rise to regional hegemony is thus threatening with the application of the Thucydides Trap. As Graham Allison sets forth, "when a rising power threatens to displace a ruling power, the resulting structural stress makes a violent clash the rule, not the exception" (2017, p. xv). Although a potential war between China and the United States would most likely take place in the South China Sea, 5G is proving to be a powerful tool capable of bringing an end to Asia's peaceful coexistence. However, understanding 5G as a technology will not be sufficient to prevent the Thucydides trap; it is essential to equally comprehend China's intentions and the cultural background that shapes Beijing's foreign policy decisions. Only with a comprehensive understanding of both aspects can differences be reconciled, and the international order saved.

In this regard, the biggest difference between China and the West is most probably the belief in two contradicting conceptions of world order. Whilst the West promulgates the existence of a set of 'universal values', Beijing persistently affirms that the Chinese civilization is unique and excluding. The PRC consequently rejects the Westphalian system of nation-states, instead promulgating the notion of the civilization-state; an exclusive form of political organization that requires specific values and organizations capable of representing China's differentiated culture (Rachman, 2019). In consequence, the main concern for the West may well be that today the nation-state is in decline.

Globalization has sparked an identity crisis and a cultural void in multiple regions, especially within Europe. On the contrary, Beijing is successfully implementing 5G technologies within the South China Sea to promote the 'made in China' *modus vivendi*, which includes its interpretation of the world order. Whilst the West is struggling to safeguard its cultural universality, Beijing is consolidating its sphere of influence in the Eastern Hemisphere; 5G is once again awakening the Middle Kingdom of Asia.

However, it is important to bear in mind that 5G is a highly fluctuating technology. This means that as 5G evolves, so will Beijing's capabilities. External factors will thus determine China's technological strategy, for better or worse. The COVID-19 pandemic, for example, is showing that Chinese 5G power is not completely unshakable. Conspiracy theories (that Huawei networks have caused the pandemic) and the international economic slowdown are set to impact the worldwide deployment of 5G, which will undoubtably delay Beijing's foreign policy strategy in the South China Sea. Although this dissertation has presented Beijing's current 5G capabilities and their impact on the international order, future studies must analyse these same capabilities in a post COVID-19 world. Furthermore, in order to better comprehend China's information strategy in the South China Sea, it will be essential to investigate the specific propaganda and disinformation campaigns launched by Beijing. Only with a true comprehension of China's 5G capabilities and intentions, can innovative and far-reaching solutions be presented to politicians in the West. However, it will be equally important for political scientists and information engineers to work hand in hand; only then can Beijing's strategy be truly deciphered and challenged.

7. BIBLIOGRAPHY

5G Americas. (2016, November). *Network Slicing for 5G Networks & Services*. Retrieved from https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_Network_Slicing_11.21_Final.pdf

5G PPP Architecture Working Group (2019, June). *View on 5G Architecture.* Retrieved from https://www.trust-itservices.com/sites/default/files/View%20on%205G%20Architecture%20-%205G%20PPP%20Architecture%20Working%20Group.pdf

Alden, C. & Aran, A. (2012). *Foreign Policy Analysis: New Approaches.* New York: Routledge.

Allison, G. (2017). *Destined for War: Can America And China Escape Thucydides's Trap?* London: Scribe.

Baños, P. (2017). *Así se domina el mundo: Desvelando las claves del poder mundial*. Barcelona: Editorial Planeta.

Bartholomew, C. (2020). China and 5G. *Issues in Science and Technology,* 36(2), p. 50-57.

Bicheno, S. (2020, February 20th). *Huawei is still the leader on 5G commercial contracts*. Telecoms. Retrieved from https://telecoms.com/502562/huawei-is-still-the-leader-on-5g-commercial-contracts/

Brown, k. (2017). *China's World: What Does China Want?* London: I.B. Tauris.

Campbell, K. et al. (2019, November). *The 5G Economy: How 5G will contribute to the global economy.* IHS Markit. Retrieved from https://www.qualcomm.com/media/documents/files/ihs-5g-economic-impact-study-2019.pdf

Cardona, F. (2009). *El Arte de la Guerra.* Barcelona: Brontes.

Cave, D. et al. (2018, October 10th). *Huawei and Australia's 5G network* (Report No. 8/2018). Australian Strategic Policy Institute. Retrieved from https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-10/Huawei%20and%20Australias%205G%20Network.pdf?wk2qurC5OGPs1DZmePkkYm_bKw8Rn5Yj

Cheney, C. (2019, July*). China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism.* Pacific Forum. Retrieved from https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf

China Daily (2019, April 9th). *Huawei's R&D investment in 2018 exceeds $15 billion.* Retrieved from https://www.chinadaily.com.cn/a/201904/09/WS5cac0859a3104842260b5265.html

Chung, M. & Mascitelli, B. (2015, October). *Strategic Positioning of Huawei on the International Political Stage.* doi: 10.4018/IJABIM.2015100101

Congressional Research Service (2020, April 24th). *U.S.-China Strategic Competition in South and East China Seas: Background and Issues for Congress.* Retrieved from https://fas.org/sgp/crs/row/R42784.pdf

Costello, J. & McReynolds, J. (2018, October). *China's Strategic Support Force: A Force for a New Era.* Washington D.C.: National Defence University Press

Cronin, P. & Neuhard, R. (2020, January 8th). *China's Political Warfare Campaign in the South China Sea.* Center for a New American Security. Retrieved from https://www.cnas.org/publications/reports/total-competition

CSIS (2016). *How much trade transits the South China Sea?* Center for Strategic & International Studies. Retrieved May 5, 2020, from https://chinapower.csis.org/much-trade-transits-south-china-sea/

CSIS (2018, October). *South China Sea Energy Exploration and Development.* Center for Strategic & International Studies Retrieved from https://amti.csis.org/south-china-sea-energy-exploration-and-development/

Doffman, Z. (2019, July 6th). *Huawei Employees Linked to China's Military and Intelligence, a Reports Claim*. Forbes. Retrieved from https://www.forbes.com/sites/zakdoffman/2019/07/06/huawei-employees-linked-to-chinas-state-intelligence-agencies-report-claims/#6f92e9334b24

Duesterberg, T (2019, December 12th). *Can We Avoid Collateral Damage in the 5G Battle with China? The Role of International Standards.* Forbes. Retrieved from https://www.forbes.com/sites/thomasduesterberg/2019/12/12/can-we-avoid-collateral-damage-in-the-5g-battle-with-china-the-role-of-international-standards/#3e676edb6fb9

Finite State (n.d.). *Huawei Supply Chain Assessment.* Finite State. Retrieved May 5, 2020, from https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf

Frankopan, P. (2015). *The Silk Roads: A New History of the World*. London: Bloomsbury.

GSMA (2017). *An Introduction to Network Slicing.* Retrieved May 5, 2020, from https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf

GSMA Intelligence. (2019, November*). Internet of Things in the 5G Era: Opportunities and Benefits for Enterprises and Consumers.* Retrieved from https://www.gsma.com/iot/wp-content/uploads/2019/11/201911-GSMA-IoT-Report-IoT-in-the-5G-Era.pdf

HCSEC (2019, March). *Annual Report: A Report to the National Security Advisor of the United Kingdom.* Huawei Cyber Security Evaluation Centre Oversight Board. Retrieved from

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

Hemmings, J. (2020, January). Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road. *Asia Policy*, 15(1), p. 5-21.

Huawei et al. (2017, February 28th). *5G Service-Guaranteed Network Slicing White Paper.* China Mobile Communications Corporation, Huawei Technologies Co., Ltd., Deutsche Telekom AG, Volkswagen. Retrieved from https://www-file.huawei.com/-/media/corporate/pdf/white%20paper/5g-service-guaranteed-network-slicing-whitepaper.pdf?la=en

Iplytics (2019, November). *Who is leading the 5G patent race? A patent landscape analysis on declared 5G patents and 5G standards contributions*. Retrieved from https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf

ISDP (2018, June). *Made in China 2025: A Backgrounder*. Institute for Security and Development Policy. Retrieved from https://isdp.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf

Ivezic, M. & Ivezic, L. (2019, April 9th). *5G Critical Infrastructure: The Most Critical of All.* 5G Security. Retrieved from https://5g.security/5g-security/5g-critical-infrastructure/

Jacques, M. (2009). *When China Rules the World: The Rise of the Middle Kingdom and the End of the Western World.* London: Penguin.

Xi, J. (2017, October 18th). *Xi Jinping: 'Time for China to take centre stage'.* BBC News. Retrieved from https://www.bbc.com/news/world-asia-china-41647872

Johnson, L. & Wirtz, J. (2011). *Intelligence: The Secret World of Spies.* New York: Oxford University Press.

Jonsson, P. et al. (2019, November). *Ericsson Mobility Report*. Ericsson. Retrieved from https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf

Kania, B. (2019, November). *Securing our 5G Future: The Competitive Challenge and Considerations for U.S. Policy.* Center for a New American Security. Retrieved from https://s3.amazonaws.com/files.cnas.org/documents/Kania-Securing-Our-5G-Future-2.pdf?mtime=20191029084132

Kania, E. (2019, June 7th). *Chinese Military Innovation in Artificial Intelligence.* Center for a New American Security. Retrieved from https://s3.amazonaws.com/files.cnas.org/documents/June-7-Hearing_Panel-1_Elsa-Kania_Chinese-Military-Innovation-in-Artificial-Intelligence.pdf?mtime=20190617115242

Kaplan, R. (2012). *The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate*. New York: Random House.

Kaplan, R. (2014). *Asia's Cauldron: The South China Sea and The End of a Stable Pacific*. New York: Random House.

Kaska, K., Beckvard, H. & Minárik, T. (2019). *Huawei, 5G and China as a Security Threat.* NATO Cooperative Cyber Defence Centre of Excellence. Retrieved May 5, 2020, from https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf

Kendall-Taylor, A. et al. (2020, April). The Digital Dictators: How Technology Strengthens Autocracy. *Foreign Affairs,* 99(2), *p.* 103-115.

Kissinger, H. (2014). *World Order: Reflections on the Character of Nations and the Course of History.* London: Penguin Random House.

Lewis, J. (2018, December). *How Will 5G Shape Innovation and Security: A Primer.* Centre for Strategic & International Studies. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf

Malik, M. (2013, May). Historical Fiction: China's South China Sea Claims. *World Affairs*, 176(1), p.83-90.

Marshal, T. (2016). *Prisoners of Geography: Ten Maps That Tell You Everything You Need to Know About Global Politics.* London: Elliott and Thompson Limited.

Martin, E. (n.d.). *The Economics and Geopolitics of Global Fisheries*. Austrian Economics Center. Retrieved May 5, 2020, from https://www.austriancenter.com/economics-geopolitics-global-fisheries/

Medin, M. & Louie, G. (2019, April). *The 5G Ecosystem: Risks and Opportunities for DoD.* Defence Innovation Board. Retrieved from https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF

OECD (2018). *China's Belt and Road Initiative in the Global Trade, Investment and Finance Landscape.* OECD Business and Finance Outlook 2018, OECD Publishing, Paris, p. 61-101. doi: 10.1787/26172577

Orwell, G. (1949). *Nineteen Eighty-Four*. London: Penguin.

Pan, J. (2019, March 27th). *Made in China 2025: everything you need to know*. IG. Retrieved from https://www.ig.com/en/news-and-trade-ideas/other-news/made-in-china-2025--everything-you-need-to-know-190327

Perez, C. (2020, February 24th). *5G Explained: The Competitive Landscape*. Foreign Policy. Retrieved from https://foreignpolicy.com/2020/02/24/5g-cellular-huawei-china-networks-supply-chain-competitive-landscape-power-map/

Perez, C. (2020, January 22nd). *5G Explained: Technology and Infrastructure*. Foreign Policy. Retrieved from https://foreignpolicy.com/2020/01/22/5g-cellular-huawei-china-networks-technology-infrastructure-power-map/

Perez, C. (2020, March 31st). *5G Explained: National Security*. Foreign Policy. Retrieved May from https://foreignpolicy.com/2020/03/31/5g-cellular-huawei-china-networks-national-security-power-map/

Permanent Mission of the People's Republic of China to the United Nations (2009, May 7th). *United Nations.* Retrieved from https://www.un.org/depts/los/clcs_new/submissions_files/vnm37_09/chn_2009re_vnm.pdf

Qualcomm (2017, August 2nd). *Understanding 3GPP – starting with the basics.* Retrieved from https://www.qualcomm.com/news/onq/2017/08/02/understanding-3gpp-starting-basics

Rachman, G. (2019, March). *China, India and the rise of the civilization state.* Financial Times. Retrieved from https://www.ft.com/content/b6bc9ac2-3e5b-11e9-9bee-efab61506f44

Riikonen, A. (2019). Decide, Disrupt, Destroy: Information Systems in Great Power Competition with China*. Strategic Studies Quarterly,* 13(4), p. 122-145.

Rogers, M. & Ruppersberger, D. (2012, October 8th). *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.* Permanent Select Committee on Intelligence. Retrieved from https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

Rugge, F. (2019). *The Global Race for Technological Superiority.* Milan: Ledizioni.

Segal, A. (2018, October). When China Rules the Web: Technology in Service of the State. *Foreign Affairs,* 97(5), p. 10-18.

Ship Technology (2018, June 19th). *Smart Ports: increasing efficiency and cutting costs.* Retrieved from https://www.ship-technology.com/features/smart-ports-increasing-efficiency-cutting-costs/

Shoebridge, M. (2018, November). *Chinese Cyber Espionage and the National Security Risks Huawei Poses to 5G Networks.* Macdonald-Laurier Institute. Retrieved from https://macdonaldlaurier.ca/files/pdf/MLICommentary_Nov2018_Shoebridge_Fweb.pdf

Singh, A. (2019, August 26th). *The Malacca Dilemma: A Hindrance to Chinese Ambitions in the 21st Century.* Berkeley Political Review. Retrieved from https://bpr.berkeley.edu/2019/08/26/the-malacca-dilemma-a-hindrance-to-chinese-ambitions-in-the-21st-century/

Smith, J. & Taussig, T. (2019, October). The Old World and the Middle Kingdom: Europe Wakes Up to China's Rise. *Foreign Affairs*, 98(5), p.112-124.

Sparks, K. et al. (n.d.). *5G Network Slicing Whitepaper.* Federal Communications Commission. Retrieved May 5, 2020, from https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/2018/5G-Network-Slicing-Whitepaper-Finalv80.pdf

Strassler, R. (1996). *The Landmark Thucydides: A Comprehensive Guide to 'The Peloponnesian War'*. New York: Free Press.

Synder, G. (2002). Mearsheimer's World Offensive Realism and the Struggle for Security: A Review Essay. *International Security*, 27(1), p. 149-173

United Nations Convention on the Law of the Sea (UNCLOS), United Nations, (1892, December).

Yap, C. (2019, December 25th). *State Support Helped Fuel Huawei's Global Rise.* The Wall Street Journal. Retrieved May 5, 2020, from https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736

Zeng, D. (2010). *Building Engines for Growth and Competitiveness in China: Experience with Special Economic Zones and Industrial Clusters.* Washington D.C.: The World Bank

World Bank (2015, July 3rd). China Economic Update. Retrieved from https://www.worldbank.org/content/dam/Worldbank/document/EAP/China/ceu_06_15_en.pdf