ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Understanding the Huawei case: a cybersecurity challenge?

September 2020

Martina Gambacorta

Abstract

5G introduces new important challenges for the cybersecurity, due to the increased vulnerabilities. The suspicion on Huawei of being China-backed has driven many nations to implement specific measures in order to protect their 5G network infrastructures. While considering this frame, it is argued that the Huawei case has been largely debated for strategic concerns, but not for technical ones. Specifically, three of the Five Eyes Intelligence—US, Australia and UK—have opted for banning Huawei from the country's 5G infrastructure. In the case of the US-China trade-war reasons seem to be strongly political and commercial. Australia is mainly driven by geopolitical concerns, due to the fear of China's presence in the Pacific area. The UK initial position was merely commercial, until the Government shifted from considering Huawei potential risks as mitigable, to respond to the US pressure on its allies and replicate the US ban on Huawei. With regard to the EU, the Toolbox of risk mitigating measures proposes a softened approach that has merits, being able to bring together geopolitical, commercial and national security concerns. EU Member States—and some non-EU countries—should decisively pursue the measures suggested and break a standoff that resembles that of a Cold War between US and China.

CONTENTS

INTRODUCTION

5G is the Fifth Generation of wireless mobile technology that will be able to provide greater data speeds, lower latency, and simultaneous connectivity of different devices. 5G will result in an advance in robotics and automation, virtual and augmented reality, and artificial intelligence and machine learning–that will exponentially increase the traffic of data, the massive reliance on the Internet of Things (IoT) and the use of the latter in critical infrastructure. Therefore, a higher resilience on the 5G infrastructure will inevitably bring about new security threats and cybersecurity challenges that will aim at preventing espionage and cyberattacks, fully conscious that risks cannot be completely mitigated. Also, the risk of known or potential vulnerabilities that might be exploited by certain actors with mala fide intentions will have to be considered. In that regard, Chinese's company Huawei Technologies Co. Ltd is on the spotlight: it has become a crucial player in the global market because of the technological and commercial advantage, but the legal and political influence of the Chinese state on this technology industry does not reassure. The Chinese National Intelligence Law of 2016 requires companies to support and cooperate in the national intelligence work and China has publicly claimed to have an adversarial perception of the West, and a willingness to build a stronger global influence while pursuing its National Superiority Agenda that—among all—has largely based on cyber espionage. Moreover, international law seems to be devoid of any real power able to constrain Huawei. Confidence building is also a no viable solution in the short term: given the lack of any binding nature or any mechanism to ensure compliance, existing approaches have provided limited predictability and no lasting remedy, bringing about very little change in behavior.

Thus, the known capability and inclination of China that raised from the past activity in which Huawei was supposedly involved, suggests that 5G deployment is more than a technocratic matter and a comprehensive approach should recognize that the issue has both economic and national security implications. This is not to say that Huawei should not be considered technically speaking. Much of the policy debate has been missing the technical aspect and policy makers should consider it in an evidence-based discourse for or against Huawei. It is often argued that Huawei 5G equipment might allow Huawei and/or the Chinese government to access to that network and to execute espionage or military missions, but no concrete evidence is provided, at least publicly. Therefore, Finite State has embarked on a large scale study of the Huawei cybersecurity-related risks. Through its proprietary technology platform, more than 1.5 million files embedded within 9,936 firmware images from 558 different products were analyzed to check for risks including hardware backdoor credentials, insecure software practices, and the presence of known and 0-day vulnerabilities. In fact, Huawei provides almost all the components of 5G infrastructure: solutions for the core and radio access network or even tools and services to support 5G site planning, radio propagation analysis, and power consumption planning. The supply chain of a telecommunication equipment is drastically complex. Huawei, for instance, claims 150 global suppliers in the supply chain. In such a long chain of hardware, software, and service providers any component might contain critical vulnerabilities or backdoors that could be exploited; to secure them is to understand the complexity of the supply chain itself and assess its security vulnerabilities. The

results of the analysis show that Huawei devices quantitatively pose a higher risk than comparable devices from other vendors, and, moreover, updates are not improving the security of the devices.

Given this, the paper will organize as follow: chapter 1 illustrates the facts that has made Huawei a global challenge; chapter 2 presents Huawei products security vulnerabilities that emerges from more general challenges that a supply chain can pose, and measures that should be implemented to mitigate the risk; chapter 3 gives concrete example of different governmental responses—namely those of three of the Five Eyes Intelligence; finally, chapter 4 exposes the softened approach, evidence-based promoted by the EU toolbox of risk mitigating measures.

In this sense, the current study significantly contributes to the debate in several and important ways. The Huawei case has largely been politicized, to the extent that many nations have imposed a ban on the company in order to pursue a trade war, to asses geopolitical concerns or to preserve strategic alliances. Conversely, I will argue that the softened EU's approach has merits and should decisively be pursued by EU Members States that still found themselves in a standoff that resembles that of a Cold War between US and China. In an era where hacking and espionage are being increasingly common, nor an American vendor or a Turkish one could be fully trusted. The EU's approach, however, is a valid solution to bring together geopolitical, commercial and national security concerns.

1. HUAWEI AS A GLOBAL CHALLENGE

1.1 5G: a new generation

As the connected future is pursued, the 5G race has become both a geopolitical and a security concern. 5G is enabling the digital economy of the future characterized by a lightning-fast internet connection; it is connecting billions of devices as part of the internet of things (IoT), and is allowing to realize transformative technologies like autonomous vehicles, telemedicine and unforeseen innovations. The evolution from 4G to 5G is advantaging both consumers and multiple industries. Global mobile data traffic are expected to grow eight times by the end of 2023, that is why a more efficient technology is needed. In this sense, these networks will be able to address the capacity needs from the growing mobile data traffic, while industries will base on new capabilities brought on by 5G. Due to its innovations, three are the specific areas of use. First of all, the enhanced *mobile broadband* ables to address traffic growth demands and higher consumer needs. For instance, the digitalization of enterprises increasingly requires human-centric usage of connectivity, such as access to multi-media content, 4k streaming on a mobile device or on-site live experiences. Second, the massive increase of the *IoT*, namely a network of physical objects, devices of all type and sizes, vehicles, smart phones etc. all connected, communicating and sharing information based on stipulated protocols with the aim of smart reorganizations, positioning, tracing and even personal real time online monitoring, online upgrade, process control and administration. 5G guarantees connectivity for millions of devices, while transmitting a low volume of non-delay-sensitive data thanks to a low bandwidth and not latency critical. Finally, the deployment of *critical IoT*, that refers to more efficient and innovative services used by a range of industries for the

reliably meeting time-critical communication needs. 5G allows an ultra-reliable, resilient and instantaneous connectivity as well as stringent requirements on availability, latency and throughput. Given the ubiquitous nature of this network, reliance on it will inevitably increase to the extent that critical industries—transportation, energy, manufacturing, communication—will rely on it. As a consequence the possibility of espionage or cyber attacks will increase too, and the national security might be at stake.

1.2 Why Huawei?

Huawei is a big telecommunications equipment distributor and consumer electronics manufacturer, with headquarters in Shenzhen, Guangdong, China. Ren Zhengfei— previously a military technologists in the People's Liberation Army—founded the company in 1987, then expanded across more than 170 countries. Huawei has rapidly become the world's largest telecoms company and the second-largest smartphone company, behind Samsung, able, today, to supply servers, semiconductors, entire smart city and surveillance solutions. Among all Chinese companies, Huawei is thought to be particularly tied to the PRC security apparatus. The UK's Intelligence and Security Committee claimed a lack of transparency in its financial structures. CIA blamed the Party for the same reason. Motivations exist for the Chinese government to support the company, and due to authoritarian nature of the state, the Party has the capability to do so. Huawei receives a special treatment through soft loans that reached more than US $30 billion before 2011, and increased thanks to two state controlled banks, China Development Bank and China Import an Export Bank. The Chinese attitude is confirmed by the countless low-interest loans to different developing countries to be spent on Huawei equipment such as data centers in Zambia, fiber projects across Africa and smart cities and surveillance projects in Kenya and Pakistan. Then, it has been reported a high degree of overlap between the personnel of the company and the apparatus:12,000 of Huawei's 160,000 employees are party members.

1.2.1 Technological and price advantage

The rise of Huawei is parallel to the Chinese national policy of technological superiority: it is the largest telecoms equipment manufacturer and, unlike its adversaries[1], it can produce 'at scale and cost' all the elements of a 5G network. This allows Huawei and other Chinese telecommunications companies to have a visible and active role in the development of global 5G standards as well as to acquire a significant proportion of core patents for 5G. It is estimated that the 10% of the '5G-essential' industrial property rights in radio access solutions is held by China. Moreover, Chinese influence in the global standards organizations (ITU, 3G Partnership Project) is increasingly growing as it is demonstrated by the key positions held by Chinese representatives. Of course, the growth of Chinese technology companies in the global market is the result of

[1] Other Chinese telecommunications companies have noticeably contributed to the development of global 5G standards while acquiring a significant proportion of core patents for 5G. 5G equipment and services is provided for the 10% by Chinese companies, with Huawei and ZTE at the top. Also, China is increasingly influencing the global standards organizations (ITU, 3G Partnership Project) due to the key positions of some Chinese representatives.

the governmental industrial policy: Huawei's affordable pricing is a result of the preferential treatment of domestic providers, which control 75 percent of the Chinese market.

1.2.2 National superiority agenda and operations of influence

The determination of the People's Republic of China to become a digital technology superpower dates back to China's 2006 long-term national innovation strategy that supposed the efforts of the government through focused investment into technology research and development. Security concerns, as well, around the use of Chinese technology are as old as its rising position on global markets. Its strategy of deterrence is two-sided and, as such, contradictory—from the one hand, China is hiding the maximum level of capability while from the other hand, it is giving signal of its capability to deter other states. Chinese technology companies embrace innovation and quality while maintaining affordable costs, and for this, they occupy a significant position in the global market. However, Western countries perceive the legal and political influence of the Chinese state over its companies as threatening. China has implicitly declared its adversarial perception of the West, and has been seeking a stronger global influence that made use, among all, of cyber espionage practices. As a result, Western government officials and the security community are concerned with the possibility of Chinese companies to be deployed by the Chinese government with mala fede intentions. In fact, China has a bad reputation for persistent industrial espionage, especially for several Chinese technological companies having targeted academia, industry and government facilities with the aim of collecting secrets in the economic and political sector.

1.2.3 Legal and political frame in China

With the Chinese National Intelligence Law of 2016, companies are required to support and cooperate in the national intelligence work, while the state is supposed to provide protection of them. At the same time, the 2014 Counterintelligence Law claims some obligations for the most relevant organizations and individuals that are demanded to provide information, facilities and other type of assistance. Considering the relationship between technological companies and the Chinese government, private companies are likely to be used as vehicles for espionage. And in fact, the Czech NCISA assessment notes that companies usually do not refrain from such cooperation.

The difference between the Chinese and the Western approach to individual rights is also a matter to discuss. The EU position strictly acmes at protecting individual privacy and restricting mass surveillance (i.e. the General Data Protection Regulation (GDPR) and several judgments by the European Court of Justice), and—together with the United States—the EU has implemented a solid intellectual property protection policy. Conversely, the Chinese national policy clearly serves state interests over private ones.

1.3 International constrain on Huawei

Vis-à-vis this frame, what is lacking—or pretty weak—is a proper judicial or public oversight to constrain the Chinese state willing. There are no international actors charged with attribution of cyberattacks, assessment of retaliatory actions against the perpetrators and prevention of accidental retaliation against innocent targets. Developing universal rules, or laws governing the cyber governance present a very challenging problem for worldwide actors and most of the actual efforts have been unsuccessful. Roots have to be found in the core definition of sovereignty, defenses, and legal systems that differentiate in societal norms. For instance, acts of espionage within the country of operation are punishable under domestic law[2], but espionage is not directly addressed in international law—apart from specific acts such as a cyber operation that violate sovereignty or constitute prohibited intervention. As well, a state obstructing another state from exercising its sovereignty constitutes violates international law. However, to qualify cyberoperation as violation of sovereignty, the degree of infringement on the territorial integrity and the presence of interference with inherently functions of the target state is to be considered. Also, the nature and degree of state inclusion in the operation is determinant for the activity to constitute a breach of international law. Merely identifying an exploitable vulnerability in Huawei network, has little significance from an international law perspective. In this regard, applicable international law and treaty regimes to constrain China's behavior do not offer security assurances to Western governments.

To boost confidence-building, the UN promote state restraint in resorting to the use of cyber tools for malicious operations and encourage cooperation between states in order to reduce the risk of misunderstanding and miscalculation in cyberspace. Most of the recommendations aim at preventing harmful ICT practices, enhancing the exchange of information and the coordination and cooperation between participating states. The norms and confidence-building measures (CBMs) proposed by the UN found application in the Organization for Security and Cooperation in Europe (OSCE), G7, G20 and the EU, but the lack of any binding nature, any mechanism to ensure compliance indicates that existing approaches have provided limited predictability and no lasting remedy, bringing about very little change in behavior.

Alternative avenues have been explored too, even if not pertaining to standard conflict-prevention measure in cyberspace. While coupling cyber-related negotiations with a broader political dialogue, the US, China and Russia concluded bilateral cyber agreements in an effort to de-escalate mounting political conflicts. For instance, against the growing accusations to China in 2015, which concerned its economic cyber espionage operations in the US, President Barack Obama and Chinese President Xi Jinping defined a 'common understanding' on curbing such activities: both leaders committed that their governments would not knowingly support the cyber theft of corporate secrets and business information. Although the hopes were high, the validity was to be proved, and in fact, just a year after the agreement was signed and amidst an unfolding trade war, the US accused China of violating the agreed rules.

[2] For instance, an exclusion of Huawei from domestic could be assessed for disproportionality.

2. HUAWEI PRODUCTS SECURIT Y

2.1 Past activity and product security

Given the aspects previously considered, Huawei has faced significant criticism related to the security risks of its products, resulting in many western governments ban on the company. Nevertheless, the same governments have never made available the technical concerns on Huawei vulnerabilities basing their discourse merely on geopolitical and legal issues. In order to provide a context to the current debate on Huawei security risks, the company's past activity must be narrated. In fact, the company has been repeatedly blamed for industrial espionage, the 2003 Cisco case[3] and the 2014 T-Mobile lawsuit[4], and for violation of international economic sanctions against Iran and North Korea, particularly significant given that Huawei uses components produced in the US. Then, the company is actually being investigated by the US for fraud and theft of intellectual property. Australian intelligence reports in 2018 indicated that Huawei personnel were used to access codes to infiltrate foreign networks. In January 2018, the African Union's Ethiopia headquarters saw data exfiltrated from its network every night for five years and then sent using Ethio Telecom, whose network was built by Huawei and ZTE. The Chinese government had primarily funded the African Union headquarters, while a company owned by the Chinese state had built them and described them as a 'gift.' Canada and Poland have detained two Huawei officials, one related to the US investigations mentioned above (involving Huawei's chief financial officer, daughter of the founder and president of Huawei) and the other on grounds of espionage. Of course, Huawei rejected all these accusations. Given the rejections, spying reports could only but underline the 'potential' of Chinese government espionage operations. The NSA planted backdoors in Cisco's products for years, and so could could do the PLA. In May 2019, Dutch intelligence agency AIVD found backdoors on Huawei equipment belonging to a Dutch carrier and worked to determine whether or not they were used for spying by the Chinese government. Vodafone—the European biggest phone company—also found backdoors in some Huawei products' software and denounced the possibility of Huawei unauthorized access to carrier's fixed-line network in Italy, responsible for providing internet service to millions of homes and businesses. This occurred after 2011 Huawei promises to remove backdoors and security vulnerabilities in home internet routers. After that, Vodafone identified additional backdoors in the optical service nodes—parts of its fixed-access and responsible for transporting internet traffic over optical fibers and broadband network gateways, which allow subscriber authentication and access to the internet. In July 2012, during a presentation at Defcon, Felix Lindner and Gregor Kopf denounced several critical vulnerabilities in Huawei routers to announce that they uncovered several critical vulnerabilities in Huawei routers (models AR18 and AR29) which could be

---

[3] Cisco, an American company leader in IT, networking and cybersecurity, accused Huawei of industrial espionage and copy of data codes and serial numbers used in routers. Cisco also claimed that Huawei copied Cisco's technical documentation and Cisco's text in Huawei's user manuals for routers and switches. Moreover, Cisco charged Huawei for having copied Cisco's command line interface (CLI) and the corresponding screen displays. It was a case of unlawful copying of intellectual property. Huawei did not immediately respond to the inquiries. 20 months later, the lawsuit resulted in agreements between the two companies. The competition of the lawsuit comes a review of of Huawei's product and after Huawei stopped the sale of products at issue. Also, Huawei agreed to change its command line interface, user manuals, help screens and portions of its source code to address Cisco's concerns.

[4] T-Mobile accused Huawei for stealing Intellectual property by stealing parts of a smartphone testing robots called Tappy, and copying operating software and design details. Huawei admitted that two employees acted inappropriately, while disagreeing with the larger trade secrets claimed in the case. However, the jury actually charged Huawei and awarded T-Mobile with $4.8 million.

potentially exploited to remotely access the device. Also, Lindner and Kopf criticized a certain lack of transparency in Huawei security issues.

The 5G infrastructure has many components and Huawei provide almost all the solutions for the core[5] and radio access network[6] or even tools and services to support 5G site planning, radio propagation analysis, and power consumption planning. The supply chain of a telecommunication equipment, however, is drastically more complex. Huawei, for instance, claims 150 global suppliers in the supply chain. In such a long chain of hardware, software, and service providers any component might contain critical vulnerabilities or backdoors that could be exploited; to secure them is to understand the complexity of the supply chain itself. Cybersecurity become harder when users cannot trust vendors; nevertheless, regardless of intent, security vulnerabilities remain.

2.1.1 Supply chain security challenge

Hardware attacks are the most devastating attacks of the supply chain attack surface. There are no confirmed backdoors in hardware that are currently being deployed but in recent years security researchers have warned of the power and stealth of a potential compromised hardware. Nonetheless, suspicion and speculation largely accuse government of being involved. Edward Snowden accusations against the NSA are emblematic. In fact, attacks of this kind are hard to detect and no software for cyber defense can truly overcome an hardware backdoor, not even patch it after detection. Backdoors can also be found on firmware and software that have emerged as the attack surfaces of choice due to the difficulty in being detected. Attacks can have many forms, for instance, using a known and default username and password to a device. Moreover, the continuous update of firmware and software makes the issue even more challenging. One of the most challenging aspects of supply chain security for devices is that the supply chain does not end the moment a device is placed on the network. The regular update is supposed to patch vulnerabilities, but at the same time it can completely change the software of the device so that —without a strong security regime imposed by the equipment manufacturer —developers or or suppliers could insert malicious code into a firmware that could stay undetected. In 2014, the Russian threat actor group known as Energetic Bear applied this same technique to target several software of the Industrial Control Systems (ICS) destined to critical industrial and energy networks. As a result, more than 250 companies were affected.

2.1.2 Huawei devices vulnerabilities

Given this, the policy debate has focused on the assumption that Huawei equipment in 5G networks may allow Huawei and/or the Chinese government to access that network for espionage or military missions. Nevertheless, no public proof has never been released by any intelligence agency or government body. Finite

[5] The central part of the 5G infrastructure, for new functions related to multi-access technologies

[6] Responsible for the connection of individual devices to other parts of a network through radio connections

State[7] has embarked on a large-scale study of the Huawei cybersecurity-related risks. Through its proprietary technology platform, more than 1.5 million files embedded within 9,936 firmware images from 558 different products were analyzed. Given the supply chain challenges previously mentioned, the analysis aimed at detecting risks including hardware backdoors, unsafe use of cryptographic keys, signs of suspicious software development practices, and the potential presence of 0-day vulnerabilities. Technical analysis cannot prove malicious intent; however, backdoors were found in 55% of the total tested devices, on average 102 vulnerabilities were known, while substantial evidence proves that 0-day vulnerabilities were abundant. To sum up, Huawei devices appeared highly compromised, more than other vendors' devices. Moreover, Huawei claims increasing security and transparency, while this study showed that updates were actually decreasing them.

The weak security posture and the high number of vulnerabilities in Huawei devices should primarily drive policy makers. After that, the risk assessment process must consider the geopolitical and legal environment related to the country's infrastructure and suppliers.

2.1.3 Risk mitigation

These conclusions lead to ask whether or not it is possible to manage the risk. If the right amount of resources are applied, it is always possible to mange risk. There are examples of supply chain security efforts that are emblematic. The UK Huawei Cyber Security Evaluation Centre (HCSEC), founded in 2010, is probably the most comprehensive approach aimed at securing the telecom supply chain. The objective is the mitigation of perceived risks that arise from the involvement of Huawei in the UK critical infrastructures; it evaluates and reports security evaluations of a range of Huawei devices of which the source code are acceded and verified.

5G can be deployed securely, and the improvement in lives and society that it will lead to, will be safe. Of course, the risk of a cyber attack cannot be completely eliminated. However, a comprehensive supply chain risk-mitigating network plan, constantly monitored, can enormously minimize risks. The first step is verifying the security posture of the devices. Firmware analysis, for instance, can provide a clear and secure image of the company, against potentially politically charged accusations. The firmware can be analyzed through automated analysis tools. Every device should be analyzed, in oder to understand exactly what devices make part of the network and how they are being configured. Firmware verification and network monitoring agents can be deployed inside the endpoint, in order to report software information, patch levels, running services etc. Monitoring must be passive and constant over time, rather than periodical. More generally, it is crucial to understand the organization's supply chain and model contracts with partners in order to conduct independent security tests and corresponding security updates. In that regard, transparency directly bring about a better security assurance.

---

[7] Finite State is a cybersecurity agency with backgrounds in the US Intelligence Community. Headquartered in Ohio, its aim is to protect the devices by finding vulnerabilities and threats with the supply chain.

In this sense, governments—and thus customers of the 5G equipment—should pursue a risk management approach by developing a proper cybersecurity protocols. For instance, it should include constant behavioral analysis of many device through advanced machine learning algorithms that can compare those device to baseline models of that device, its firmware, and its category. The following step is then the establishment of a dialogue with vendors that aims at sharing the findings and patching potential vulnerabilities.

3. FROM A TRADE-WAR TO A STRATEGIC ACTION

3.1 Understanding the Huawei Ban: the Five Eyes

This frame has led many western states to discuss about the eventual ban of Huawei from the build-out of 5G infrastructure. Specifically, as Huawei embarked on major projects, the Five Eyes—an Anglophone intelligence alliance between Australia, Canada, New Zealand, the United Kingdom and the United States — focused a great amount of interest in Huawei. While the UK and Canada, appeared incline to manage cybersecurity risks, the US and Australia, were determined to eliminate them. This latter approach is clearly the most straightforward if considering national security factors only, but the calculation becomes complicated if taking into consideration geopolitical and economic factors.

3.1.1 The US and the trade-war

The story of US vs Huawei dates to 2008 with the US barring Huawei from buying 3Com and parts of the wireless division of Motorola. In 2010 Huawei and ZTE were excluded from Sprint from telecommunication contracts while in 2011 Huawei participation in the US National Emergency Communications Network project was denied. During the Obama administration Ralls Corp—owned by executives of China's largest machinery manufacturer Sany Group—was banned from owning four wind farms in Oregon. The common thread was ‘national security concern’. In 2012, the long standoff during the Obama ‘pivot to Asia’[8] resulted in Huawei and ZTE being adjudicated as a ‘security threat’ to the US. In 2018, Huawei was growing at an astonishing pace, Donald Trump’s attitude was to combat China and its unfair trade practices. That was the beginning of the still-ongoing US-China trade war. It concerned politics, tariffs, and international law, while also touching on intellectual property theft. In May 2019 Trump introduced Huawei on the Entity List, which includes all the companies unable to do business with any organization that operates in the United States. A week after a 90-day reprieve kickstarted the Huawei ban which could make arrangements until August 19, 2019. This 90-day reprieve was extended three consecutive times. On February 2020, the US government issued a final 45-day reprieve: the Huawei ban would have taken full and permanent effect by April 1, 2020. In the previous months, ARM Holdings announced the definitive ban on Huawei, in order to comply with all the regulations assessed by the U.S. government. This resulted in a halt for Huawei in the access to current and future chip designs and similar breaks from Google and Microsoft. A total blockade on the company’s US partners.

[8] It was a yearlong congressional investigation into Huawei and ZTE, provider of telecommunications equipments.

Being a main supplier of network infrastructure, concerns about Huawei have firstly focused on cell towers rather than on cellphones. Any hard evidence of backdoors in Huawei's cell towers was found, but probably, there was no need. The risk was too high and Huawei was to be excluded from the most sensitive components of the 5G infrastructure installed on American soil. Cell networks were potential target for Chinese espionage, thus creating a high risk of Chinese surveillance agencies using them to put malware into the network, whether through Huawei or not. In this sense, the ban on android and other components seemed more a trade issue rather that a security one. Of course, just the lack of smoking-gun evidence of a company manipulating hardwares of foreign government could not be decisive enough to ban that company's equipment in 5G networks. However, the company's past activity could not persuade certain foreign governments and leverage their perception of the risk. This may explain why Western governments broadly perceived Huawei as a security risk, and why they differed on the management and the mitigation of that risk.

3.1.2 Australia and geopolitical concerns

Australia was the first state in the Five Eyes intelligence alliance that, in August 2018, obliging its telecommunication carriers to not purchase 5G equipment and services from Huawei. Canberra did not provide a detailed technical explanation to support its decision, and it was unclear whether the choice came from a geopolitical concern or a security threat. The presence of Huawei in Australian 5G networks is not likely to significantly alter the risk of current Chinese espionage, as the risk is already high. 5G may only slightly increase the probability of sabotage and its consequences. Huawei's exclusion may only slightly reduce vulnerabilities.

Australia's decision on the Huawei ban from its 5G networks caused a hostile response in China, since it was the first worldwide. It followed an increasingly complex debate within Australia about China's security intent and actions, that included the issue of 'territorial expansionism' and influential attitude on the Australian domestic politics. Then, the Telecommunications and Other Legislation Amendment Act 2017 entailed obligations on carriers to protect the confidentiality of communication of telecommunication networks and facilities from the risk of espionage and sabotage in time of war or crisis. All technical arguments were dismissed, namely that Huawei equipment could be safely used in the periphery of the network—or edge—while excluded from the sensitive core. Conversely, it was argued that 5G design supposes that sensitive functions—that are currently performed in the physically separated core—gradually move closer to the periphery of the network. Put simply, it was claimed that no distinction between core and edge really exists. In that regard, traditional technical mitigation tactics would become obsolete. The debate has strongly focused on the risks of possible backdoors in hardware or programming of software that allows access to Chinese spies or saboteurs. Nevertheless, the debate did not consider that Chinese spies and saboteurs, like their US and Russian counterparts, have myriad of other alternatives to access Australian communications content and infrastructure. For instance, the Stuxnet attack on Iran's nuclear programme occurred through German equipment; Chinese attacks on Australia have been delivered by exploiting vulnerabilities of commercial software such as Microsoft. Moreover, 5G cannot be uniquely internal to Australia. Internet-based services

such as Facebook, Google or Netflix are being provided by servers in other countries, which means that 5G systems will communicate with and rely on Huawei-equipped networks in Indonesia, Singapore, China and South Korea. To give an example, China is collaborating with the International Civil Aviation Organization, and its members, for the integration of 5G technologies—Huawei-equipped—into aircraft. Once aircrafts enter Australian airspace, they will be unavoidably connected to Australia's air-traffic control systems. Given this, China could be able to access Australian communications despite the fact that its companies do not have primary contracts for the country's 5G network equipment. In that regard, cyber espionage should be managed through specific cybersecurity strategies, even if—it must be said—the risk of sabotage is harder to mitigate. However, cyber disruption or sabotage of a network in a 5G environment are not that straightforward. Mobile networks are part of larger and complex telecommunications infrastructures. Huawei Chinese-backed attempts of sabotage would have limited effectiveness, or could even fail.

3.1.3 The UK and new challenges for the cybersecurity

In 2011 the UK government established the Huawei Cyber Security Evaluation Centre (HCSEC) to face potential risks of Huawei's involvement in UK critical infrastructure. HCSEC evaluates the security of Huawei products introduced in the UK telecommunications market and develops new tools and techniques to guarantee security in the telecommunication. The Centre has often found certain vulnerabilities but Huawei has immediately remediated, and has worked on the Huawei's basic engineering and security processes and code quality, resulting in a more secure Huawei product.

On March 2019, the HCSEC published the Huawei Cybersecurity Evaluation Centre oversight board annual report addressed to the National Security Adviser of the United Kingdom stating that the board can "provide only limited assurance that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK" (Original report, 2019). Moreover, the report has highlighted that much of Huawei's software "lacks basic engineering competence" and "significantly increased risk to UK operators", and that some coding practices are hard to audit and could only be managed by "developers... actively working to hide bad coding practice rather than fix it" (Original report, 2019). Finally, HCSEC warned that "it will be difficult to appropriate risk-manage future products... until the underlying defects in Huawei's software engineering and cyber security processes are remediated..."(Original report, 2019), and that the board "has not yet seen anything to give it confidence in Huawei's capacity to successfully complete ... its transformation program that it has proposed as a means of addressing these underlying defects."(Original report, 2019).

Anyway, the HCSEC identified 3 main risks to the UK's 5G infrastructure:

1. The loss of availability—as a taking down—of one or more mobile networks may cause a knock-on impact to the country and wider economy due to the inability of people to communicate.

2. The absence of end-to-end trustworthy[9] components to build a secure and resilient 5G infrastructure

3. The possibility of an undetected attack targeting the confidentiality or integrity of messages traveling over the UK's 5G networks

Despite this, the UK initially took the decision to not ban Huawei; the decision was not surprising and factors were mainly commercial and political. First of all, UK's mobile operators significantly influenced the Government during the process. Second, a Chinese ambassador statement—according to which exclusion would have led to worse economic and political relations—may explain a certain fear of retaliation. In this sense, the choice appeared to be driven more by political factors rather than technical: accepting high risk vendors in the 5G network was risky because it hindered moving towards OpenRAN and other interoperability-driven initiatives, which aim at avoiding a dependency on the same vendor of 4G and 5G radio equipment—a lock-in scenario the UK was in. In this sense, technical advantages were easily sacrificed for political ones. However, the Government's decision was heavily justified by the premise that security risks could be mitigated by new cybersecurity tools.

Of course, alternatives to Tier-1 suppliers exist, and these present independently supply chain options. However, they have never been considered and to some extent, this makes the problem commercial and not technical. 5G RuralFirst project in the Orkney Islands proved that new, innovative equipment can be deployed for mobile networks in many challenging environments possible, while working without existing handsets and equipment. These options might diversify the supply chain. Again, this was a commercial challenge which required commercial incentives to be addressed: a mobile operator will aways opt for the lowest cost solution to maximize the profit.

This initiative finally arrived. Given the limited assurance provided by the HCSEC and the commercial incentives the UK Government is willing to provide, the Government lastly opted for a ban on Huawei. After 31 December 2020, all the mobile operators will not be able to buy new Huawei 5G equipment. Reversing a January decision that gave the company a limited role in the building of 5G infrastructure, Huawei is asked to remove all 5G networks in the UK by 2027.

Digital and Culture Minister Oliver Dowden justified this decision by claiming that US sanctions imposed on the company in May had changed the landscape. Costs and technological delay is not a UK concern anymore. Huawei provides much of the UK's telecommunications infrastructure, including 4G and the ban will need investments in removing them for a total of £2bn and two or three years of delay. Then, replacing them will cost £500m over 5 years. Sale of Huawei smartphones, however, was not affected. "There's no such thing as a perfectly secure network," Media Secretary Oliver Dowden told the House of Commons and the U.K. had to make sure its system was "as secure as it possibly can be". But many agree that the decision is becoming

[9] The end-to-end is a network design in which the application specific features are located at the communication end points, in contrast to features located at intermediate points, such as gateways and routers. In end-to-end method, intermediate nodes pass data randomly, making it possible to replace any intermediate node with any other one without failure of functions, since functions exist only in end points. Critical components are removed from intermediary communications nodes allowing increased routing options, improved data delivery rates and making sure applications only fail if the end point fails.

politicized, more related to the U.S. trade friction with China than real security concerns. Not by chance the decision was taken after Prime Minister Boris Johnson attempted a compromise to placate both Beijing and Washington. London has been a US ally for decades, but five years ago it initiated a "golden era" of engagement with China. This standoff was finally concluded with a win for Trump.

4. A CYBERSECURIT Y APPROACH

4.1 The EU 5G risk assessment

Before the UK ultimate decision, European allies were taking a similar approach to the UK claiming to be far from a ban. The EU is supporting member-state governments to assess and mitigate risks associated with vendors and supply chain, basically implementing the approach suggested by Finite State.

Huawei, from its part, has welcomed and interpreted the EU coordinated 5G network security risk assessment as an important step towards a cybersecurity-base, evidence-based approach that analyzes risks rather than targeting specific countries or actors. The company has also claimed its availability to collaborate with European partners in order to build a safe and fast connectivity for Europe’s future needs.

4.1.1 The EU toolbox of risk mitigating measures

The EU toolbox of risk mitigating measures has been released on January 2020, as part of the bloc's drive to roll-out 5G by the end of 2020. On February 11, the pragmatic approach suggested was concretized from one of the Member States: the ruling Christian Democratic Union of Germany published a paper on 5G mobile networks that did not mention any total ban on suppliers, against any form of protectionism under the pretext of national security and in favor of free trade. Conversely, technological progress was promoted in order to mitigate risks related to the supply chain.

To sum up, the toolbox requires Member States to apply common security requirements such as identifying suppliers and build a trustworthy relationship based on transparency, developing technical cybersecurity tools and eventually applying restrictions on high-risk suppliers from key assets considered to be critical and sensitive—thus rejecting the Australian point of view— and finally, and diversifying vendors. Also, the toolbox assures Member States that they will be provided with all the tools to ensure the security of the 5G infrastructure and supply chain such as telecoms and cybersecurity rules, EUstandardized certifications, trade defence instruments, EU funding programmes and investments. Europe is now among the most advanced regions to launch 5G services by investing 1 billion, of which 300 million in EU funding. Through the Recommendation on Cybersecurity of 5G networks of March 2019, the Commission called on Member State to complete a national risk assessment to be transmitted to the Commission and the EU Cybersecurity Agency. In November 2019, the European Union Agency for Cybersecurity (ENISA) supported this objective through a report that identified the main threat and threat actors, the most sensitive assets and vulnerabilities/risks. Then,

the Commission required Member States to implement the measures recommended in the toolbox by 30 April 2020 and to work on a joint report for the implementation in each Member State by 30 June 2020.

The EU's approach represents a softened but meritorious road that should decisively be pursued by EU Members States that still found themselves in a standoff that resembles that of a Cold War between US and China. In fact, Member States position is not so clear. Following the UK's Huawei ban, France is adopting a de facto ban on Huawei. German telecommunications regulator has implemented some additional security requirement that impose high standards for the 5G installation, that have been argued to be a de facto ban. Given the supposed Huawei case of espionage, Polish government has stood toughly against Huawei and has signed an agreement with the US that will likely functionally ban Huawei. Italy— the only major Western European country to sign on to China's Belt and Road Initiative—initially installed Huawei equipment in Vodafone's 5G until lawmakers actually decided to apply the Golden Power[10] constraining Huawei's role in 5G. These examples well show that EU Member States are still premature in considering Huawei in geostrategic, commercial and national security terms.

The Huawei-US standoff will evolve rapidly and unpredictably in the near future, and until that moment doubts will exist on whether some EU Member States will cease to the US pressure. Trump administration is supposed to escalate tensions with China. The problem is that the US will retaliate if Member States choose Huawei. Conversely, China will retaliate if they pose a ban. This is why EU governments—and some non-EU countries—should well implement the European Commission's common 5G risk assessment, that does not call on any ban, but takes into account both technical and non-technical factors. By following its recommendations, individual countries might be able to constrain China and US ability to threaten retaliation.

At the moment, despite the US pressure, the likelihood of European countries to adopt a zero-tolerance policy toward Huawei is every low. Economic interests mostly move them towards this position: they are apparently the first factor to consider. For instance, EU-Huawei relationship determine the access of European companies —Nokia and Ericsson—in China.

CONCLUSION

The objective of this paper was to provide a framework that may help readers understanding the policy challenges that surround the Huawei company, and that have lead to what has been defined 'the Huawei case'. The debate that developed over it represents a standoff for many nations, divided between siding the US position of a total ban on cell towers and cellphones and trusting the Chinese rejections of any accusation of cyberthreat. Evidence has broadly suggested cybersecurity and espionage risk associated with Huawei, but all the debate can only evolve around the 'potential' of Chinese government espionage operations. Given the uncertainty, the international response is incredibly diverse, ranging from pursuing trade-wars, to prefer

[10] Special power through which the Government can require operators to notify contracts for the acquisition of goods and services and then veto the acquisition or impose security requirements for the implementation, that will be subject to specific monitoring; as well, companies of specific sectors may be provided with support for detection, mitigation and eradication of specific threats.

geopolitical and strategic concerns, to implement a high-stand cybersecurity approach. In that regard, this paper supported the comprehensive and softened approach promoted by the EU toolbox of risk mitigating measures that aims at uniting members of a regional area behind a common and positive attitude based on an extraordinary level of cybersecurity, while maximizing the economic and technological potential of 5G.

All the things considered, these conclusions still rise some implications that the future research must deeply investigate. While illustrating the Australian approach and the EU's one towards 5G-equipment providers, a controversy in their point of view emerged around the distinction of the 'edge' and the 'core' functionalities. To deliver reduced connection latency, 5G networks is designed to function more at the edge rather than at the core of the network. Australian's position rejected the idea that Huawei equipment could be safely used in the periphery of the network—or edge—while excluded from the sensitive core, a position that the EU namely sustained. Conversely, Australia claimed that 5G design supposes that sensitive functions—that are currently performed in the physically separated core— gradually move closer to the periphery of the network, meaning that excluding vendors from supplying equipments to the most sensitive parts of the network may be a useless solution.

However, a broader question should address whether a ban on Huawei could be a long-term viable solution, given that it jeopardizes economic and commercial concerns and does not really address national security interests. Concerns of sabotage and espionage have to be addressed and mitigated, but a ban on Huawei from the implementation of 5G, would not be such effective. China would be able of espionage with or without the Huawei equipment. APT1, APT3 and APT10, which stand for "advanced persistent threat", are some of the most famous hacker groups that are related to the Chinese-party state and that since 2014 have extensively increase their activity of espionage for economic, political and military purpose. Moreover, the main attack vectors have been spear-phishing and social engineering, and not mobile communication infrastructures. This means that all 5G networks have to be securitized. More effective and appropriate feasible paths are preferred to address 5G network security concerns: network security must be improved; transparency and security are needed in the race to 5G independently from who is providing 5G equipment; cybersecurity must take a proactive approach.

REFERENCES

Anonymous, *Statement on the EU coordinated risk assessment of the cybersecurity of 5G networks, Huawei press release*, October 2019

Anonymous, *EU continues its wavering attitude toward Huawei*, Global Times, July 2020

Anonymous, *ENISA threat landscape for 5G networks: Threat assessment for the fifth generation of mobile telecommunications networks (5G),* European Union Agency for Cybersecurity, November 2019

Anonymous, *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*, NIS Cooperation Group, CG Publication, January 2020

Anonymous, *Finite State Supply Chain Assessment*, finitestate.io, January 2020

Anonymous, *Secure 5G networks: Commission endorses EU toolbox and sets out next steps,* European Commission press release, January 2020

Barnes J. E. and Santriano A. U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist, The New York Times, March 2019

Depsey J. Judy Asks: Should Europe Ban Huawei's 5G? Carnegie Europe, Judy Depsey's Strategic Europe, January 2020

Dutta A.and Marek J. A Concise Guide to Huawei's Cybersecurity Risks and the Global Responses, The National Bureau of Asian Research (NBR), October 2019

Gill J. and Parrock J. *EU still have work to do to beef-up 5G security ahead of European rollout*, Euronews, July
2020

Goel S. *How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race*, Connections: The Quarterly Journal

Gold H. *UK bans Huawei from its 5G network in rapid about-face*, CNN Business, July 2020

Lecher C. and Brandom IS HUAWEI A SECURITY THREAT? SEVEN EXPERTS WEIGH IN, The Verge, May 2019

Mascitelli B., Chung M. *Hue and cry over Huawei: Cold war tensions, security threats or anti- competitive behavior?*
Science Direct, May 2019

Moss S. *Understanding the Huawei ban*, datacenterdynamics.com, May 2019

Kaska K., Beckvard H. and Minárik T., *Huawei, 5G and China as a Security Threat*, NATO COOPERATIVE CYBERDEFENSE CENTRE OF EXCELLENCE, 2019

Kelion L. Huawei 5G kit must be removed from UK by 2027, BBC News, July 2020

Kleinhans J., *5G vs. National Security: A European Perspective*. Berlin: Stiftung Neue Verantwortung, 2019

Pawlak P., Tikk Eneken, Kertunnen M. *Cyber conflict uncoded: the EU and conflict prevention in cyberspace*, European Union Institute for Security Studies, April 2020

Rhode B. *Australia, Huawei and 5G*, ISS, Strategic comments, Volume 25 Comment, October 2019

Rühlig T. & Björk M. *What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe*, THE SWEDISH INSTITUTE OF INTERNATIONAL AFFAIRS, 1/2020

Scott B. *How Huawei is dividing Western nations*, featured article on Techcrunch, March 2020

Spacey J. *What is Network Infrastructure?* Simplicable, March 2018

Shoebridge M. *Chinese Cyber Espionage and the National Security Risks Huawei Poses to 5G Networks*, MacdonaldLaurier Institute, November 2018

Smith A. After months of U.S. pressure, U.K. bans China's Huawei from its 5G network, NBC News, July 2020

Tabuchi H. *T-Mobile Accuses Huawei of the Theft from Laboratory*, New York Ties, September 2014