The European House Ambrosetti

Novembre 2019

5G and security in Italy
An overview of problems and possible remedies

white paper

1. EXECUTIVE SUMMARY

Introduction

5G will be a revolution: a new Internet. Designed to be used for a multitude of vertical markets, it must have the capability to serve very different needs like high capacity, low latency, extreme reliability, high energy efficiency and all the combinations of these.

5G will change the economy and create a huge value by boosting productivity increase: the total mobile business will grow from $3.9 trillion in 2018 to $4.8 trillion in 2023. It will enable a whole new world of opportunities, amongst others: remote surgery to save lives in difficult geographic areas, intelligent manufacturing with machines that may optimize their own actions and communicate their knowledge to the other machines. This would give a possibility to manage a higher flow of traffic in a safer manner, to improve the security management in towns, to refine the remote services for elder people, to boost AgriTech, Tourism and many other sectors. All with very different needs in term of network usage, from the high speed with low latency performance needed in remote surgery or autonomous driving, to most IoT applications where energy efficiency is the key as there will be a multitude of devices in remote locations that must work for long periods without maintenance.

In order to be able to serve such different needs, 5G will need a network capable of reconfiguring itself autonomously, to "feel" traffic and application needs, to be "virtualized". Together with the fact that the number of connected devices will be huge, it makes the 5G network more exposed to cyber-attacks. Because the applications that 5G enables are critical (e.g. autonomous driving, remote surgery, intelligent manufacturing etc.), 5G security issue is a hot topic: the struggle for world supremacy today is a technological one and the battlefield will largely be the 5G network where, for example, companies will manage their innovation, data, manufacturing and knowledge, and countries their security.

The issue

The key issue in 5G is the current lack of a reasonable business case, which makes it difficult for operators to meet the 5G coverage required by governments. This despite the fact that the total mobile telephony market plus the productivity improvements driven by the 5G, is worth $4.8 trillion (2023 forecast).

The key implication is to understand all the economic and non-economic drivers of vendors and of their Nation States, while selecting a 5G technology provider.

The battleground for 5G infrastructure is Europe: China is an impenetrable market for Western companies and Chinese vendors are banned from the US. It is in Europe that vendors will fight to find the returns on their investments, economic or otherwise.

5G, like electric cars, smartphones, robot and AI systems, is a deep technology, i.e. through them a vendor or a Nation State can go deeply into the client's system, be it another Nation State or a Company. For this reason, it is extremely important to conduct a thorough assessment of the governance system and the policy framework of vendors along with the relation they have with their Nation State's political system. Chinese vendors have a leading position in 5G technology, and they have had some security issues in the recent past. Furthermore, Chinese vendors have not been able to clearly demonstrate their full independence from the Chinese State in the past (2011).

Within this context, Huawei is a fast-growing and successful company, with a revenue CAGR of 20% over the last 6 years with a unique, almost dominant position along the whole supply chain of the 5G and their systems are not interoperable with those of other vendors.

Conclusions

5G will greatly transformed the way the business is done. This represents a huge threat and an equally huge opportunity. There are 3 key messages that we want to convey on 5G security:

1. **There is a new level of security risk** –5G has a significant increase in the vectors of attack and risk of greater negative impact for the economy and society if the attacks are successful.

2. **The geopolitical aspect of the risk is crucial** – The legal frameworks in non-EU countries do not always grant that States cannot exert undue influences on vendor companies.

3. **A country can increase its GDP by tackling of the 5G security issue** – Becoming an inherently trustworthy ecosystem would create a better business environment and foster investments. Not doing it, can have significant costs in terms of industrial espionage and systems' disruption.

Recommendations for Italy

Europe and its Member States, including Italy, need an inherently trustworthy 5G infrastructure if they want to grow and prosper attracting investments. This implies to go beyond the pure cybersecurity aspect of the issue, to consider the potential drivers of all vendors, economic and geo-political and to audit their supply chain even before designing cybersecurity counter measures.

We recommend to Italian Policy Makers (PM) and Industry Players (IP) to deploy the following 3 measures, with the key objective to create an Italian 5G system that is inherently trustworthy:

1. **An assessment of its critical infrastructures** (1, 2, 3 priority level) – PM, IP

2. **A process to audit the whole supply chain of the vendors** – PM, IP

3. **The establishment of a COE - Centre of Expertise for threat intelligence** where processes and experiences are continuously shared with like-minded countries and bring to augmented capability – PM, IP

In conclusion, looking at 5G security it is extremely important to take a holistic approach. There are two points: firstly, the 5G security is not purely related to cybersecurity issue; geo-economy shall be considered as an integral part of the role that 5G plays in the increasing economic competition between Nation States and economic blocs, especially between US and China. Secondly, cyber risks

are defined in a very technical way, looking at cyberattacks and backdoors. The correct approach would be to look at the evolution of our entire digital world and how social networks can influence the public opinion.

2. WHAT IS 5G AND WHY IT IS SO IMPORTANT

2.1. 5G is not just a faster 4G

Why do we need 5G? Because 5G is the answer to avoid a crisis due to the over-success of mobile. It is not an evolution of 4G, but a profound rethink and a revolution. It needs imagination to understand it or, at least, enough imagination to figure out a world in which the same happened to cars.

Each person, including newborns, would have an average of 1.1 cars. However, a car for everyone is not enough. Then, in 5 years, everyone will have at least three cars and use it every day. Traffic problems? No, because at the same time everyone will move in highways one hundred times larger. No matter if 80% of the traffic is made by ever-larger trucks and the same mid-August traffic can happen on any day and at any time of the year. Is it a problem? No, with a special permit it will be guaranteed a road is passable at top speed without ever touching the brake. But top speed will be 30 to 50 times faster than before. Impossible? Not with a new car concept 100 times lighter, 100 times stronger, and 90% more efficient than that of five years back.

The revolution of 5G is to make this dream come true on a mobile network and to sustain this growth rate for more than ten years. Nevertheless, the only way would make it possible is to complete upending every existing paradigm of a mobile network. More specifically, the new network will upgrade existing 4G networks in several ways:

- 5G networks can be 100 times faster than their 4G antecedent, with speeds of up to 10 Gbps.
- Latency will potentially decrease down to 1ms, which is 30 to 50 times better than before.
- It will be possible to have up to 1 million connections per km², 100 times more than 4G, which would be useful to support IoT.
- The network will be more than 99.999% reliable.
- Mobility will be improved, enabling connectivity on high-speed trains moving up to 500 km/h, which is about 1.5 times better than 4G.
- The radio interface will be 90% more energy-efficient than 4G (ETSI).

Meeting these market demands is very though. A rigid and inflexible network like 4G's cannot afford it. It needs a network capable of reconfiguring itself autonomously, to "feel" traffic and application needs, managing to satisfy them as fast as the thought of needing it. 5G networks can do it using software defined networks (SDN), network functions virtualization (NFV), and network slicing[1]. Those characteristics make 5G networks incredibly performing but also their complexity incomparable to that of their previous generations.

[1]Network slicing is a form of virtual network architecture using SDN and NFV. A single network connection is sliced into multiple virtual networks that can support different radio access networks, or different service types on the same radio access. Each virtual network (network slice) comprises an independent set of network functions created by software suitable for the requirements of the particular use case. Each will be optimized to provide the resources and network topology for the specific service and traffic that will use the slice. For example, a doctor can simultaneously perform an ultrasound, which requires low and constant latency with an average throughput, while downloading the patient's medical records, a task needing a high throughput, but which is insensitive to high and varying latency.

However, significant opportunities do not come at a small price. The challenge is how to meet government-mandated coverage goals, even where business justification is lacking. It has been estimated that the rollout cost for 5G across Europe would be significantly higher than for 4G, running between €300 billion and €500 billion (GSMA, 2019), an enormous commitment for European telecom operators. And this is even more true in Italy where telephone operators have paid frequencies for 5G more than €6.5 billion.

2.2. 5G use cases

Mobile phone standards up to 4G were designed to serve the needs of an infant mass market. On the contrary, 5G was designed to serve a sum of vertical markets with very different and somewhat conflicting needs. For example, some of these verticals, like virtual reality applications in maintenance of critical plant components, have the constraint of low latency and high bandwidth, no matter the conditions. On the contrary, some of IoT devices, like parking sensors, have only the restriction of low power consumption to last for years without recharging batteries, no matter the latency or the available bandwidth.

With 5G, there will almost not be discernible differences between wired and wireless connections, opening a range of possibilities that can take advantage of near-instantaneous response and high data speeds. 5G will offer to the companies blazing-fast connections and the ability to use the cloud or even multiple clouds seamlessly for computation-intensive tasks with real-time decision-making, or for retrieving all the data needed for local decision-making.

For all its features, 5G will enable an unprecedented number of applications unimaginable before.

Consumer applications

Media, entertainment and gaming will be the top consumer applications for 5G, mainly because 78% of Italians (older than 15 years old; ISTAT, 2018) already have a smartphone, and use it with increasing intensity. However, 54% of consumer expectations for 5G center on faster speeds (GSMA, 2019). So, lightning-fast browsing, downloading content faster, improved video calls, better video quality, immersive videos and instant cloud access are the top use cases for 5G enhanced mobile broadband (Qualcomm, 2017).

However, probably the most important 5G applications are still those hard to imagine, but enabled by 5G, such as immersive reality and augmented reality that can radically transform our social life that goes more and more through our smartphones. So, privacy and security will be crucial requirements for all of us.

The intense competitive pressure that telecom operators should bear, especially in Europe and particularly in Italy, makes commoditization of big investments, like 5G, a severe risk for telecom companies. They are not well equipped to manage it in consumer applications, especially in Europe.

Based on interviews with 46 Chief Technology Officers at large telecom around the globe[2], while the majority of North American telecom operators (56%) will have large scale 5G deployment before 2020, no other region is above 40%. What is the explanation of this difference? Most operators surveyed (60%) think that the biggest challenge to their 5G strategies is identifying a business case. But this was the answer of 100% of European operators and of only 11% of North American operators.

[2] Source: Grijpink, Härlin, Lung et al. (2019).

Business applications

For all the reasons mentioned above, the most likely battlefield to justify investments in 5G will be developing and managing vertical business applications.

Vertical applications	Why it is important in Italy	Economic estimate
Connected industrial and manufacturing services	Italy is the second largest manufacturer in Europe but with a problem of low productivity. Connected manufacturing can improves quality and increase productivity	$988 billion market by 2025, global[3]
The connected car market	Italy is one of the most important manufacturers in the automotive world, that is also one of the most impacting industry on our economy growth	$225 billion by 2025, global[4]
Healthcare	Italy has the oldest population in Europe and the second oldest in the world	$534 billion in 2025, global[5]
Private 5G networks in industrial and business critical environments	Italy is a very industrialized economy but is based on SMEs that should be connected to work productively	$118.5 billion in 2023 with 765.1 million devices in 2023, global[6]
Agriculture	Agribusiness sector is one of the Italian Excellences and is growing faster than other sectors	€205 billion GDP in 2018 (12% of GNP) and €41,8 billion export, global[7]
Tourism	A key sector for Italy that is losing competitiveness	10-12% of GNP in Italy[8]

Table 1. 5G business use cases

2.3. The relevance of the 5G security for national governments

The 5G security dispute is not a question of just controlling new investments

[3] Source: Million Insights.

[4] Source: Allied Market Research.

[5] Source: Grand View Research.

[6] Source: HARBOR RESEARCH (2018) *The Private LTE Opportunity for Industrial and Commercial IoT*, Harbour Research, https://www.multefire.org/wp-content/uploads/HRI_Paper_Private-LTE-Network-Paper_20-July-2017_Final.pdf.

[7] Source: La Stampa, May 2019.

[8] Source: Luiss Open.

The business of mobile telephony is huge and has an even greater influence on the whole economic system. In 2018 its direct economic impact was $1.1 trillion, about 1.3% of the global GDP. But mobile operators, like Telefonica, Vodafone or TIM controlled its largest chunk, $690 billion (61%). The stake of infrastructure providers, including tower companies, sites rent as well as electronics and technical infrastructures, was only $80 billion (7%) of which an even smaller portion falls in the business of network equipment makers, like Huawei, Nokia, Ericsson, Cisco (Figure 1). For a comparison, the business of device manufacturing was 1.5 times that of the entire industry of mobile infrastructure.

Mobile security is so important because mobile's impact on the whole economic system is fifty times bigger than the one of the infrastructure and network equipment makers.

Mobile business is important because it has a larger impact outside of the telecom business. Its impact on global productivity is $2.3 trillion, twice that of the whole mobile business. It is the value of placing an order online while waiting for someone late or receiving a timely news that require immediate reaction no matter where we are. Adding the impact on productivity to the remaining indirect economic effects, for every dollar collected by mobile operators the value created for their customers is 4 dollars. In economic terms, the global mobile ecosystem and its impacts account for almost $4 trillion, 4.6% of the global GDP, something that nobody could neglect. Plus, thanks to 5G, the average annual growth of the productivity will be the fastest growing, about 4.4% (Figure 1).

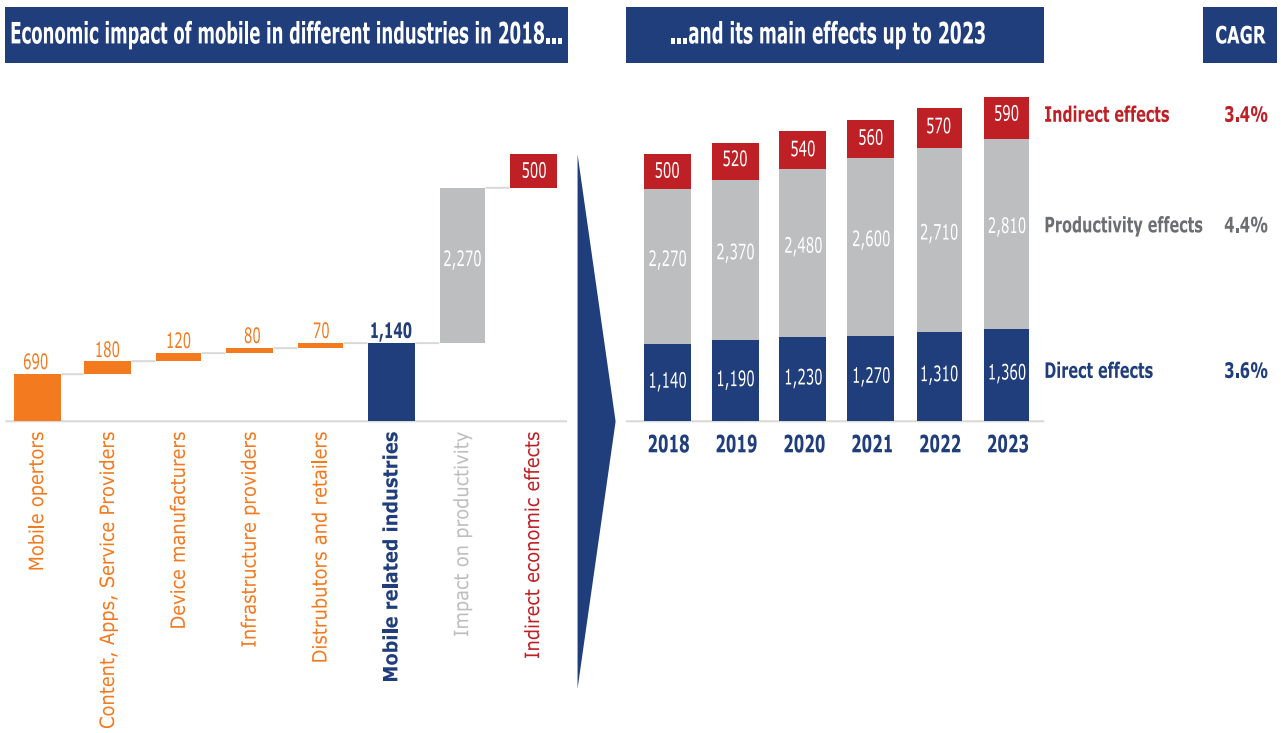


Figure 1. The global economic impact of mobile in different industries (2018-2023, billion $). Source: GSMA, 2019

The largest adoption of 5G will be in Asia. In 2025, leading the group, South Korea's 5G penetration will be 59% of total connections. It is more than in the US (50%) that will perform better than Japan (48%) and much better than China (29%).

However, the real battlefield for 5G infrastructure will be in Europe. China is an impenetrable market for Western companies and Chinese vendors are banned from the US. Nevertheless, in number of 5G connections (Figure 2), the European market will be the second largest market in the world (203

million), after China (454 million). Total connections, though, do not give a measure of the market opportunity in Europe: in the US there are 4 main mobile operators, in China 3, in the European Union 104.

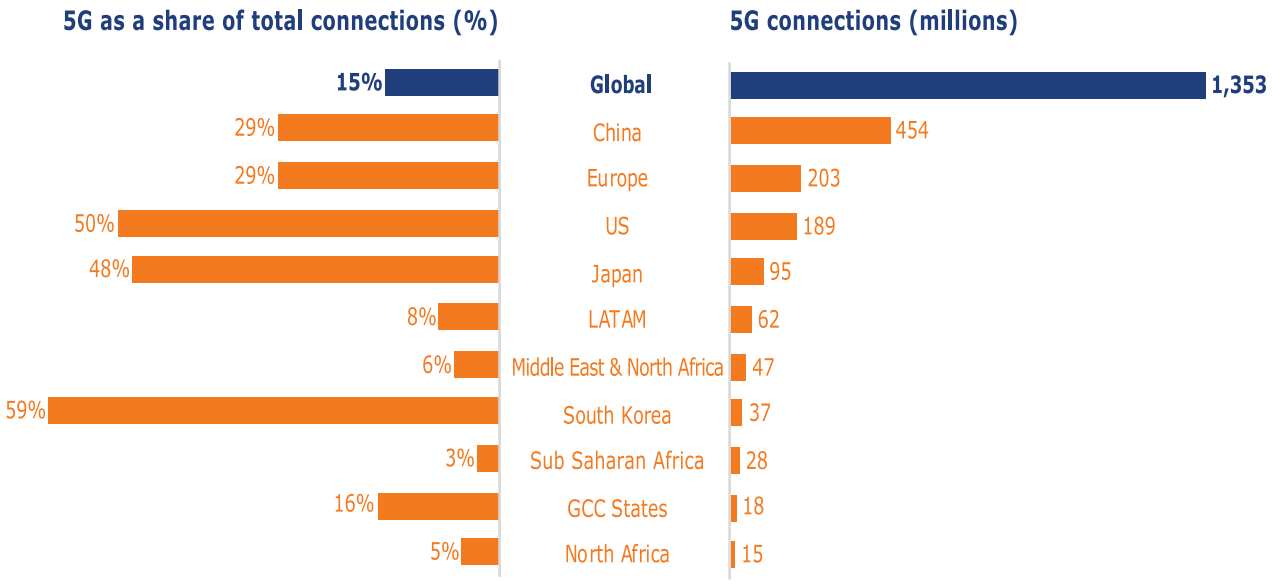


Figure 2. Adoption of 5G in 2025 as a share of total national connections and as total connections. Source: GSMA, 2019

3. 5G SECURITY: WHAT ARE THE RISKS

3.1. Mobile networks security evolution

Unfortunately, the security problems on mobile networks is nothing new. Their evolution has followed that of the mobile industry, accompanying its growth with growing concerns.

1G

1G was primarily introduced to offer mobility for voice users. Consumers started witnessing the freedom to attend and make calls while mobile. But mobile networks started witnessing serious threats and challenges immediately after its introduction. In parallel with 1G adoption and success, cell phone cloning became an industry by making and selling illegal cloned phones. Some hackers identified new ways to hijack and eavesdrop on the calls while being made and listen in to the private conversations for various nefarious reasons.

2G

With 2G, user authentication become a key focus, to reduce the call charge fraud, channel hijack and mobile cloning attack surface. The subscriber identity module (SIM) was first used to assign unique identification for mobile phones. Besides, 2G also introduced encryption on a limited scale to protect the traffic between user equipment and base station. Although it was unable to fully protect against cryptanalytics attacks, it was able to provide some basic encryption protection for signaling and user data. However, a new threat was introduced in 2G: masquerading as a carrier base station, rogue base stations were invented to intercept mobile traffic by offering fake network authentication

performing a so-called man-in-the-middle-attack. It was not the only bad news because 2G was the dawn of the mobile message spamming. It was annoying but also dangerous because spamming was used not only to send unwanted messages but also as a pervasive attack to inject false information to the mobile users and leverage on it to enable frauds.

3G

As 3G was designed to offer the next generation of data services and Internet connectivity for mobile users, new challenges and vulnerabilities were introduced to the system. To improve authentication and to protect against attacks, such as rogue base stations, 3G adopted a two-way authentication between user equipment and the network. Nevertheless, attacks such as the man-in-the-middle-attack were still possible in the UMTS environment using such tools like mobile jammers, OSMOCOMBB and slightly similar strategies. Plus, with 3G mobile networks evolved to a packet switching model, IP-based RAN (Radio Access Network) and IP Core network, and these changes released the IP-based threat vector that was not present in 1G and 2G networks.

Furthermore, as mobile devices were replaced with small-sized computers called smartphones, they became source of typical operating system vulnerabilities and weaknesses. Then, threat vector in 3G targeted mainly the user phones and their operating system. Mobile OS vulnerabilities were exploited, as mobile applications were injected with malicious code to gain unauthorized access to sensitive personal information, such as contacts, user passwords and location data.

4G

With 4G and its related evolutions, such LTE and LTE advanced, mobile networks had an incredible evolution. It was the first global mobile standard. Therefore, the most important opportunity ever to exploit the global pervasive presence of mobile communication. With 4G, threats were scattered throughout all the domains of the 4G network. Millions of malicious apps have been developed to impersonate popular apps like games, tools or banking apps. With IP core networks, 4G networks were targeted with well-designed DDoS (Distributed Denial of Service) attacks to cause a larger impact on the availability of the mobile services. On smartphones, about 87% of the time is spent using apps and at least 24.7% of mobile apps carry one high risk security flaw.[9]

However, risks on 4G are not limited to mobile users' behavior. LTE radio access networks can be exploited to gain access to device location using its Cell Radio Network Temporary Identifier, protecting the attack by encrypting the traffic carrying control signal, and command and confirm messages. LTE is based on an IP-based end-to-end open network architecture. It simplifies the network operations and reduces its costs, but on the other hand, it opens the mobile network to IP-based security threats. It helped mobile service providers offering new services and innovation, but also increased the threat vector for 4G networks. DDoS (Distributed denial of service) and APT (Advance persistent threats) were the new realities for the mobile network, as impact to the service was critical with huge financial losses as the result of such attacks. Attackers became more organized and started following a much more systematic approach in their threat execution. Therefore, it has

[9] Source: NowSecure (2016), NowSecure Mobile Security Report, https://info.nowsecure.com/rs/201-XEW-873/images/2016-NowSecure-mobile-security-report.pdf.

become harder and harder to detect their stealth presence in the mobile networks, to protect and mitigate, with an average attack consisting of months' duration.[10]

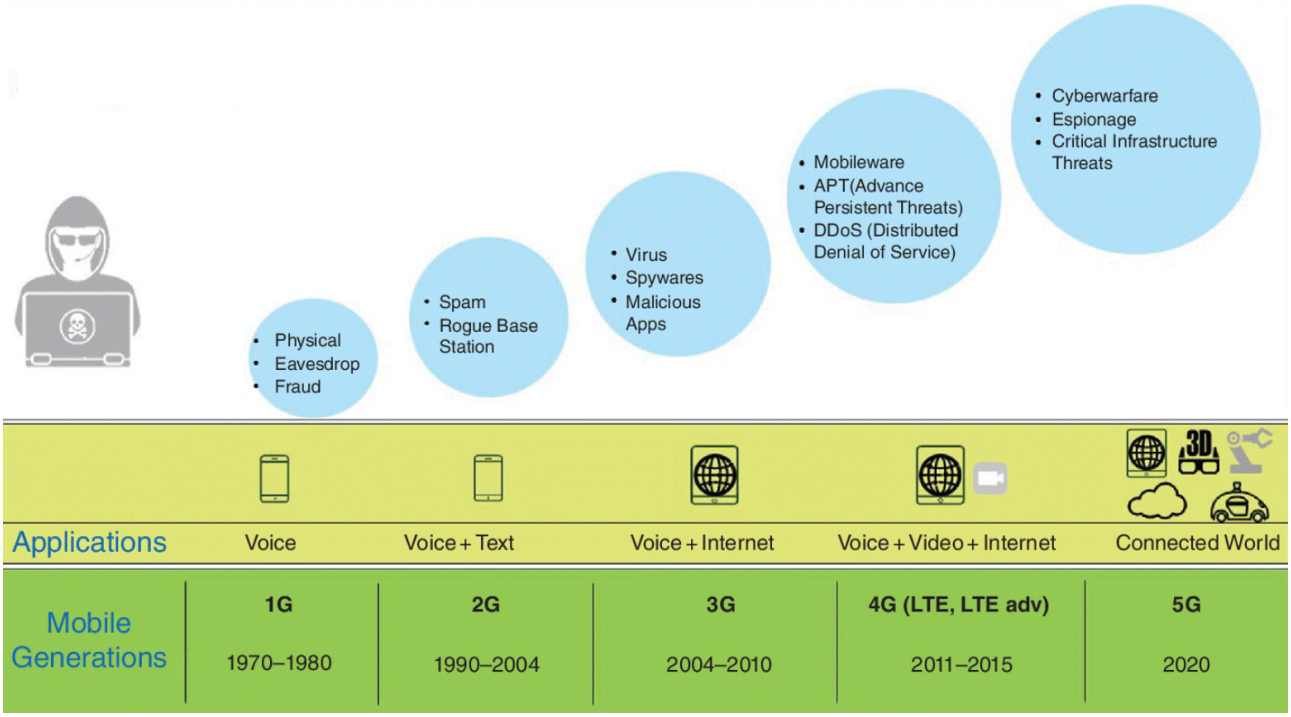


Figure 3. The evolution of mobile security landscape from 1G to 5G. Source: Liyanage, Ahmad, Bux Abro et al. (2018)

3.2. 5G networks security

Given the wide spectrum of 5G applications and services and their critical role in modern economies, as described above, motivations to threaten and attack 5G networks will be higher than in any previous network generations. It will be a main target for illegal activities driven by state-sponsored political motives, adversaries, competitors, organized crime cartels, espionage and cyberwarfare.

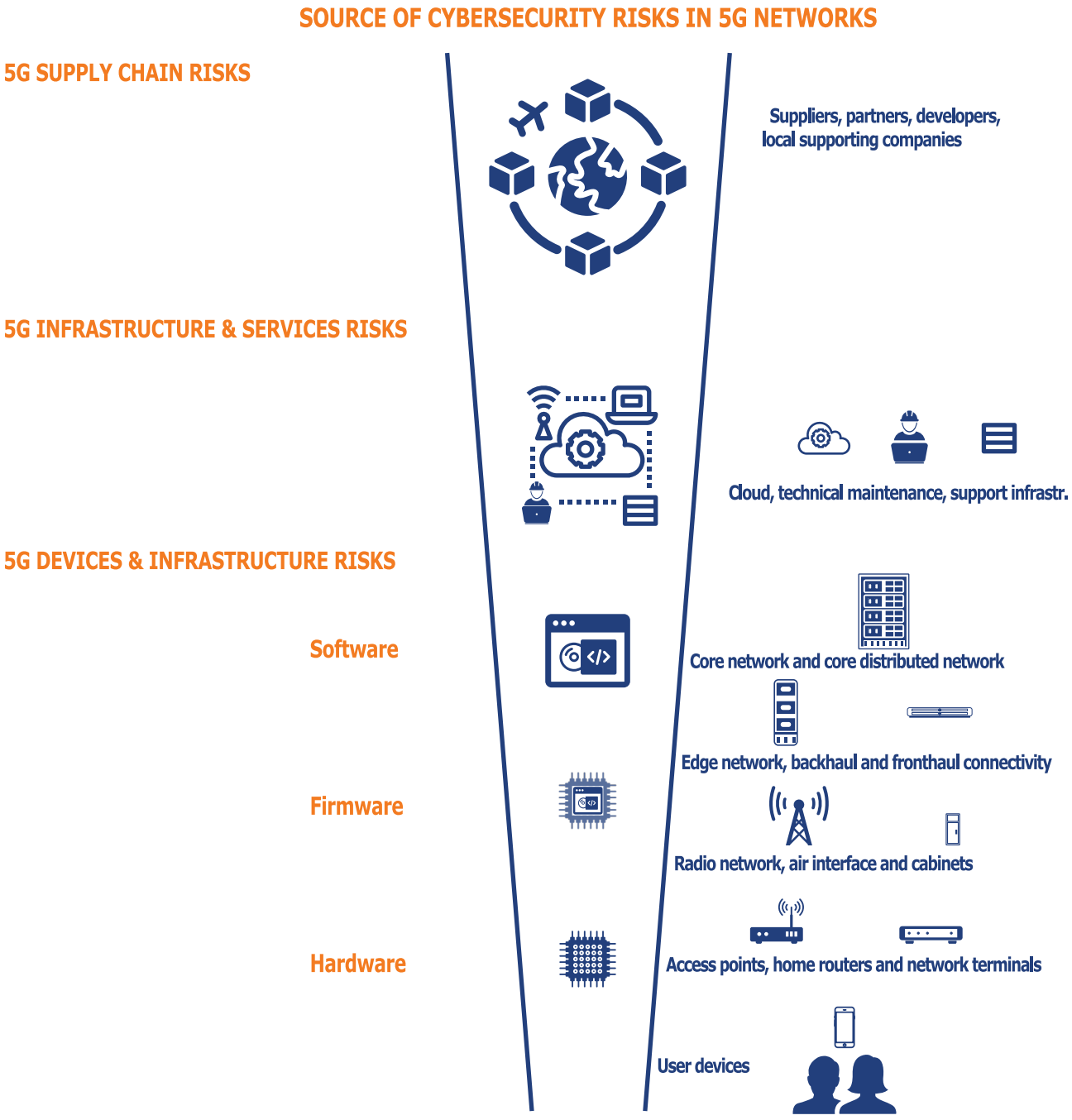
The 5G threat vector will be boundaryless, ranging from end user devices to the mobile network and its core. It includes smartphone threat types like ransomware, spyware malware and Bots. An MitM attack could be launched at the Cloud radio access domain, while DDoS may target the IP core network. Every single domain of 5G network will be under threat in such a landscape.[11] Furthermore, 5G will be a critical infrastructure connecting all the critical infrastructures, such as electricity, community health and governance, finance, trade and industrial systems.

All these elements expand and transform the threat landscape of 5G far beyond any other communication network that has ever existed. Therefore, given 5G networks complexity and its intrinsic value, 5G threats will be:

[10] Source: M. LIYANAGE, AHMAD I. et al., Eds. (2018) *A Comprehensive Guide to 5G Security*, Hoboken, NJ, John Wiley & Sons.

[11] Source: Ibid.

- Sophisticated – Complex in nature, use a multi-staged mix of various attack vectors and tools. For example, the Angler exploit kit that is packaged to exploit a multiple vendor into a single attack.
- Obfuscatory – Attacks that are obscured by multiple layers and very hard to detect.
- Evasive – Hard to detect and capable of hiding themselves, e.g. ransomware crypto-wall attack.
- Persistent – Such attacks are meant to be consistent and evolve themselves after every failed attempt.[12]



[12] Source: Ibid.

Figure 4. Sources of cybersecurity risks in 5G networks

Considering the 5G network as a complex system, risks mainly lie at three different levels: supply chains, infrastructure and services, and devices.

1) Supply chains

Opening a telecommunications equipment and looking at its components is like taking a journey into globalization. There are dozens of components: processors, memories, chipsets, integrated circuits, capacitors, resistors, batteries. They come from almost all over the world. Huawei, for example, has 150 global suppliers in its supply chain, and each of its component networks can have dozens of hardware and software suppliers. There are single components, even tiny ones, or more complex components (boards, sensors, power supply units, for example). All are conveyed in a single product and assembled based on a precise project coordinated by an OEM (Original Equipment Manufacturer), which verifies the quality of the work of the various suppliers and the characteristics of the final product.

Some of these "physical" components have a layer of software that accompanies and integrates it. It can be a microcode inserted inside a processor, a written firmware to interface hardware and software, but also drivers or another kind of software. All these software components, just like the hardware components, are inserted inside a custom software developed by the OEM to create a firmware, a software build, or an image.

However, software development is more complex to manage than hardware assembly. Each image is produced based on the work developed by dozens of companies, hundreds of development communities, and thousands of developers in sometimes very different sectors. The software development work is so specialized and interconnected that more than 80% of the software developed for a telecommunications device is reused in other devices.[13]

Thus, errors are inevitable in the development of the software image. Therefore, to have a reliable final product, it is critical to know what happens when a problem is found within the software. What typically happens is that a new software version is developed and made available to install or update – more or less – automatically.

Controlling the quality of the software is very difficult, but updating it is inexpensive. Thus, it is easier to be tolerant of software problems than of hardware problems. However, product safety depends on the solidity of both components and the interactions between hardware and software.

Furthermore, especially in 5G communication networks, where security is a crucial element, one of the supply chain suppliers may, intentionally or unintentionally, compromise the product. It is difficult to guarantee the security of a product by an attacker who knows it better than the defender.

Thus, the supply chain is the most significant attack surface for a product. That is even truer in the 5G area that has only five primary suppliers of 5G radios and hardware core networks: Huawei, ZTE, Nokia, Ericsson, and Samsung. Lack of alternatives.

Therefore, the security of a telecommunications product does not depend only on its OEM, but on its entire supply chain plus the OEM's ability to manage the security of its supply chain for each hardware and software component.

[13] Source: FINITE STATE (2019) *Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd.*, Finite State, https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf

2) 5G infrastructure and services

Supply chain security does not end the moment a device is placed on the network. It needs to be configured and reconfigured if the infrastructure changes or evolve. Telecom equipment usually has a support contract to do regular maintenance and technical interventions to fix normal problems in operations. Practically all the network devices need continuously updating their firmware and software.

Telecom network equipment is complex to install, configure, secure, update, and troubleshoot, so representatives from the vendor are best suited to service these devices. This is more and more common in Italy, where companies like Huawei sell their maintenance contracts to service providers.

This is the standard way business-to-business technology acquisition works in many industries. But, when dealing with critical networks, there are obvious security concerns associated with these services. Furthermore, in the long run, telecom providers lose their network control skills, ending up entirely depending on the vendor. For example, firmware updates in telecom networks are quite complex and often require vendor assistance. Periodically, a new "release" will be patched into the network using a combination of proprietary tools and vendor personnel who are often physically present in these events. While the risks can be managed through extensive testing, verification, and monitoring, these types of services are obvious ways that an attacker could gain access to a sensitive network and install malicious firmware updates.[14]

Updates are generally a good thing, as most firmware updates are designed to patch vulnerabilities. The most responsible OEMs will issue these patches regularly to ensure their devices are secured against newly disclosed vulnerabilities. However, each firmware update could completely change the software in the device. Without a robust security regime in place at the OEM, a single developer, a single supplier or a rogue maintenance company could insert malicious code that makes its way into a firmware image undetected. Even worse, the update servers themselves could be compromised and files modified by a malicious third-party.

In fact, this has occurred earlier this year to ASUS, a Taiwanese electronics OEM. They inadvertently sent malware to hundreds of thousands of PCs due to a compromised software update server.[15] The researchers estimate half a million Windows machines received the malicious backdoor through the ASUS update server, although the attackers appear to have been targeting only about 600 of those systems. This same technique was used by the Russian threat actor group known as Energetic Bear in 2014.[16] During that operation several developers of Industrial Control System (ICS) software were targeted in an operation that "trojaned" software updates destined for critical industrial and energy networks. More than 250 companies were affected. "These infections not only gave the attackers a beachhead in the targeted organizations' networks, but also gave them the means to mount sabotage operations against infected ICS computers," according to Symantec.

In a telecom network, support companies, maintenance partners and the whole infrastructure are part of the perimeter to secure because they are also part of the attack surface.

---

[14] Source: ibid.

[15] Source: K. ZETTER (2019) «Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers», in *Vice*, March 25, 2019-03-25, https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers.

[16] Source: N. PERLROTH (2014) «Russian Hackers Targeting Oil and Gas Companies», in *New York Times*, June 30, https://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html?searchResultPosition=1.

3) 5G devices

5G devices, including under the general definition of "device" mobile phones, RAN, edge network devices and every single component in the 5G network, are prone to hardware and firmware/software vulnerabilities.

At the hardware level, **hardware Trojans** are the gates to the most devastating attacks because they are notoriously difficult to detect. Besides no software defenses can truly overcome a hardware backdoor, and they cannot be patched after detection.[17] Their potential aims include the reduction of the reliability or even the destruction of a system, the implementation of a backdoor to leak secret information or a change of the functionality.

Hardware Trojans can be inserted at each step of the design cycle by a rogue employee or through a compromised computer-aided design (CAD) or Electronic Design Automation (EDA) tool. Trojans can be introduced by alterations of the design files in the early stages of specification design, use of malicious or compromised third-party IP vendors, alterations of the fabrication process in a third-party malicious foundry, during post-manufacturing tests and the packaging process.[18]

Hardware Trojans are challenging to identify. Even advanced post-fabrication tests cannot detect them since attackers can craft attack triggers requiring a sequence of unlikely events, which will never be encountered by even the most diligent tester. Besides, they can leverage on analog circuits to create a small hardware attack (i.e., requires as little as one gate, the dimension of a few nanometers), stealthy (i.e., requires an unlikely trigger sequence before effecting a chip's functionality) and undetectable (i.e., stores energy in capacitors siphoning charge from nearby wires as they transition between digital values[19] to not be detected by side-channel analysis).[20]

In recent years security researchers have repeatedly demonstrated the power and stealth of compromised hardware. However, they are still very complicated to detect[21], because it is expensive and/or it takes several weeks or months. Nevertheless, in the end, **every mitigation strategy for hardware Trojans requires increased control on the supply chain** (i.e., design for trust, or split manufacturing for trust).[22]

At the firmware and software level the most dangerous threats are backdoors. **Firmware and software backdoors** differ from vulnerabilities just for intentions. However, intent is very tough to prove. Then, the best intentional backdoors look like security inaccuracies and are fully deniable. So, attackers can get most of the benefits of a hardware backdoor created by a hardware Trojan, but with a smaller effort and with much more deniability.

---

[17] Source: C. DOMAS (2018) «Hardware Backdoors in x86 CPUs», in, Black Hat, July 27, https://i.blackhat.com/us-18/Thu-August-9/us-18-Domas-God-Mode-Unlocked-Hardware-Backdoors-In-x86-CPUs-wp.pdf.

[18] Source: K. XIAO, FORTE D. et al. (2016) «Hardware trojans: Lessons learned after one decade of research», in *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 22, 1, p. 6.

[19] Source: K. YANG, HICKS M. et al. (2016) *A2: Analog malicious hardware*, 2016 IEEE symposium on security and privacy (SP), IEEE.

[20] Source: S. BHUNIA, HSIAO M. S. et al. (2014) «Hardware Trojan attacks: threat analysis and countermeasures», in *Proceedings of the IEEE*, 102, 8, pp. 1229-1247.

[21] Source: N. VASHISTHA, LU H. et al. (2018) *Trojan Scanner Detecting Hardware Trojans with Rapid SEM Imaging Combined with Image Processing and Machine Learning*.

[22] Source: K. XIAO, FORTE D. et al. *Hardware trojans: Lessons learned after one decade of research*.

If a backdoor is inserted in firmware, it is typically undetectable from the operating system or applications running on the system (i.e., endpoint security software). Given that thousands of developers may contribute to a final firmware image, it is also notoriously difficult to discover where in the supply chain a backdoor was inserted.[23]

Firmware and software backdoors can take many forms. One of the simplest backdoors is adding a known, default username and password to a device. Despite its simplicity, it is quite a common one. One example is the Mirai botnet DDoS attack in 2016, which co-opted 600,000 devices with backdoor accounts into a botnet that generated hundreds of Gbps of artificial traffic to shut down entire sections of the Internet. here are many other backdoor techniques seen in a variety of other devices. In 2013, D-Link routers were found to contain a backdoor allowing remote access by setting a browser's user agent string to "xmlset_roodkcableoj28840ybtide".[24] In 2018, four different models of Android phones were found by the German government to have an unremovable backdoor[25] and, from a recently disclosed Vodafone's report, in 2011 were found backdoors in Huawei's home gateways and larger network devices.[26]

5G devices are the easiest target for a cyber-attack. In a landscape populated by millions of Internet of Things devices, connected using thousands of network devices in a software defined and virtualized 5G network, the attack surface is enormous and attack strategies could be very tough to detect. It is not possible to control everything, but **anything that is firmware or software is more likely to be attacked**.

4. SOURCE OF RISKS IN 5G NETWORKS

There are two aspects of risk: one technical and one related to policy framework.

4.1. Technical aspect: 5G networks will be more vulnerable to security breaches

The sheer number of connected devices, all with low security posture is the issue. 5G networks will be less centralized than current networks, with more sensitive network activity occurring in a multitude of locations closer to users[27], therefore, there will be new vectors of attack possible, for example:

- Distributed caches – Denial of Service (DoS) can cause major disruptions to services that require ultra-low latency, like autonomous cars or video caching. In this scenario, since a very large number of caches would be deployed at the edge of the network to cater for a large number of subscribers using low latency applications, attackers will be able to overwhelm these caches with request for content not likely to be used by non-malicious users.

---

[23] Source: FINITE STATE *Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd.*

[24] Source: J. KIRK (2013) «D-Link issues fixes for firmware backdoor in routers | Computerworld», in *ComputerWorld*, December 3, 2013-12-03T05:51-05:00, https://www.computerworld.com/article/2486450/d-link-issues-fixes-for-firmware-backdoor-in-routers.html

[25] Source: C. CIMPANU (2019) «Germany: Backdoor found in four smartphone models; 20,000 users infected», in, June 6, https://www.zdnet.com/article/germany-backdoor-found-in-four-smartphone-models-20000-users-infected/.

[26] Source: D. LEPIDO (2019) «Vodafone Found Hidden Backdoors in Huawei Equipment», in *Bloomberg*, April 30, 2019-04-30T06:45:12.877Z, https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment

[27] Source: D. STRUMPF AND CHERNEY M. (2018) «Australia's Actions Against Chinese Firms Ignite 5G Security Debate», in Wall Street Journal, September 12.

- New interfaces – Entirely new vectors of attack will result from the fact that 5G network core components will have a larger exposure to third-party application and external interfaces, because they will be virtualized and sliced to meet the needs of the different use cases.

In short, the multitude of devices connected[28] give many possible points of entry for an attacker who may use any non-critical device, typically with low security posture, as a weak entry point into a business-critical space. Such access can allow attacks via modification of data (data integrity), data exfiltration (confidentiality) or to disrupt the network (availability). It can also be used to persist in order to launch further attacks.

It is easy to understand the consequences of a malicious attack when we have fleets of self-driving cars or fully automated power plants or when Intellectual Property / sensitive information is exchanged amongst colleagues via email or messages.

4.2. Policy framework: companies' governance in China

Equally important is the policy aspect of the 5G security issue. The approach to policy framework in China is very different than the one in Western democracy, we can say culturally different. In 2011 Huawei invited a delegation from the US Congress to their headquarter in order to try and address the mounting concerns about how they managed security. The bi-partisan delegation investigated both Huawei and ZTE and found that there was no system, process or procedure in place that could prevent the Chinese Government to impose actions on Huawei and ZTE; more specifically, none of the two companies:

- Has been able to show written information on their formal or regulatory relationships with China State authorities.
- Has given specific details on China People Party's role in the companies.
- Has given detailed information on their activities in the US. Huawei, specifically, has not completely explained their company organization, history, ownership, operations, financial decisions and management.

Finally, and more importantly, none of the two companies has been able to show written evidence supporting the answers given to the commission.

The above findings have been confirmed by a work made by HJS in their assessment of the UK approach to 5G security: based on documentable sources, HJS found that Huawei is not a private company («Huawei is absolutely not a private company» said Prof. Christopher Balding, in a HJS paper and based on official Chinese documents)[29] and that they are subordinated to the 2017 National Intelligence Law, which means that Huawei is obliged to assist China's intelligence agencies in operations and research and development, even if, it must be told, Huawei claims the contrary.

[28] There will be billion of devices on which to place backdoors. Ecipe – European Center for International Political Economy estimates that 26 billion devices are going online soon. A backdoor, in cybersecurity terms, is a method of bypassing security controls to access a computer system or encrypted data. While backdoors can be common in some network equipment and software because developers create them to manage the gear, they can be exploited by attackers.

[29] Source: BALDING, C. AND OTHERS (2019) *Who owns Huawei*, Henry Jackson Society, https://henryjacksonsociety.org/members-content/who-owns-huawei/.

5. AT THE HEARTH OF THE 5G SECURITY DISPUTE

5.1. China: innovation hungry nation

The rise of China as a great industrial and exporting power is one of the truly world-changing economic events and one of the most important transformations of our time. In the late 1970s China accounted for a tiny portion of the world's industrial production and less than 1% of its trade. China became a member of World Trade Organization (WTO) in 2001 with a GDP that was one third of Japan's. By 2007, China's GDP was the world's third largest, in 2009 it surpassed that of Japan and became the world's 2nd largest economy.[30] Since 2014, China has been the world's leading manufacturing nation, and its biggest exporter. In 2018, China's GDP was $13.6 trillion, 3.4 times that of Germany and the value added of its manufacturing reached 30% of the world, about 1.5 times that of the entire European Union.

This transformation was the result of many factors, including opening China's economy to foreign investments and modernizing its economy. Foreign Direct Investments (FDI), which had run at $2 to $3 billion a year in the 1980s, exploded after the second wave of reforms launched in 1992 by Deng Xiaoping's so-called Southern Tour to relaunch economic openness, peaking at $45 billion in 1997, accounting for nearly one-sixth of all fixed investment in China. Much of this FDI went into creating an export manufacturing controlled by foreign firms. Between 1990 and 2001 China's exports more than quadrupled, from $62 billion to $266 billion, and by the end of that period more than half of the country's exports were produced by foreign firms. Foreign firms' share of high-tech exports peaked at near 90 percent in 2005 and has since fallen to around 70%.

This was a weakness for Chinese economy. In United States, Germany, and Japan the largest part of exports was produced by domestic firms. In global supply chains China's role was principally that of the "The World's Factory", the «final assembly point for products put together out of components made elsewhere or made by other foreign firms in China».[31] To reduce the dependence of China exports from foreign companies controlling the core value of products only assembled locally, in 2006 Hu Jintao (General Secretary of the Communist Party and President of the People's Republic of China) and Wen Jiabao (Premier) declared that China should become an *innovation-oriented nation*. In the same year the China's State Council issued new guidelines for the national medium- and long-term program for science and technology development (2006-2020)[32] and launched the so called "Indigenous Innovation" policy (*zizhu chuangxin*), setting challenging goals:

1. A Research and Development (R&D) expenditure at 2.5% of GDP.
2. By 2020, at least 60% of the country's development should be contributed by science and technology.
3. China reliance on foreign technology to decline to 30% and below.
4. The number of patents granted to Chinese nationals expected to rank in the top-5 globally.

---

[30] L. LI (2018) «China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0"», in *Technological Forecasting and Social Change*, 135, 2018/10/01/, http://www.sciencedirect.com/science/article/pii/S0040162517307254, pp. 66-74.

[31] Source: A. R. KROEBER (2016) *China's Economy*, New York, Oxford University Press.

[32] Source: THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA (2006a) «China issues science and technology development guidelines», in *Gov.cn*, February 9, http://www.gov.cn/english/2006-02/09/content_183426.htm. A synthesis is THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA (2006b) «The National Medium- and Long-Term Program for Science and Technology Development (2006-2020) - An Outline», in *Gov.cn*, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf.

5. A focus on 11 major sectors, including "information industry", in «order to resolve some outstanding problems bottlenecking the country's economic and social development».

The policy, supported by growing emphasis and incentives in the 11th, 12th and 13th Five Year Plan, included «subsidies for R&D in priority high-tech industries, rewards for filing patents and creating technical standards, encouragement for domestic firms and government offices to buy Chinese-made products, and, most controversially, stronger requirements for foreign companies to transfer key technologies to local firms as a condition for being allowed to invest in China».[33]

In March 9, 2015 China officially launched the "Made in China 2025" initiative during the annual plenary meeting of the National People's Congress. The main objective of the plan was to further strengthen China's position in advanced tech initiatives, transforming the country in a «world manufacturing power from the workshop of the world» (Li Keqiang, Premier of the State Council of the People's Republic of China).[34] The plan was the answer to China being no longer the lowest–cost labor market, squeezed by newly emerging low-cost producers such as Vietnam, Cambodia, and Laos. Meanwhile, China was not yet one of the top players in the high-tech arena, dominated by the US, Germany, and Japan.

The 10-year guideline was officially issued by the State Council on May 19. It was the first part of a longer (34 years) three phases plan. During Phase One (2015-2025), China is going to strive to be included in the list of global manufacturing power countries, owning and controlling the intellectual property of original products designed and conceived in China, able to challenge the incumbent leaders. In Phase Two (2026-2035), the country will rise to the medium level in the world's manufacturing power camp. Finally, in Phase Three, from year 2036 to 2049, when China celebrates its 100-year anniversary, China should be a leading manufacturing power in the world. The plan targeted 10 industries of which information technology was the first.

To support this growing effort, since 2015 China has set up 40 national and 48 provincial funds that provide funding, intellectual property, materials, M&A and other strategic assistance, including to those working on the 5G technology (Table 2).[35] China's public financial effort is impressive. It actually started in 2014 and committed $287 billion in four years, outpacing the total of Venture Capital investments in the United States in the same period ($279 billion[36]), more than four times Venture Capital investments in Europe ($66 billion[37]).

[33] Source: A. R. KROEBER *China's Economy*; ibid.

[34] Source: THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA (2017) «Building a world manufacturing power — Premier and 'Made in China 2025' strategy», in *Gov.cn*, January 31, http://english.www.gov.cn/premier/news/2017/01/29/content_281475554068056.htm.

[35] Source: S. GUPTA, COLLINS B. et al. (2019) *5G Leadership: Huawei in Context*, Barclays Research, 5 June.

[36] Source: PwC; Thomson Reuters; NVCA.

[37] Source: Dealroom.

Fund name	Fund Bn ¥	Funds-of-funds Bn ¥	Total Bn ¥
Shenzhen Guidance Fund		100	**100**
2010		**100**	**100**
China Culture Industry Investment Fund	20		**20**
2011	**20**		**20**
National Integrated Circuits Industry Investment Fund	139		**139**
Shangdong Private Equity Investment Guidance Fund		10	**10**
Silk Road Fund	265		**265**
2014	**404**	**10**	**414**
Haihe Industry Guidance Fund		100	**100**
Jilin Government Industry Investment Guidance Fund		10	**10**
Shenzhen Futian District Guidance Fund		10	**10**
Tianjin Industry Innovation Guidance Fund		20	**20**
Xiamen Industry Guidance Fund		10	**10**
Xinj iang Uyghur Autonomous Region PPP Government Guidance Fund		100	**100**
Yangtze River Industry Fund		200	**200**
2015		**450**	**450**
Beijing Big Data Industry Investment Fund	10		**10**
Chengdu Qianhai Industry Guidance Fund		40	**40**
China Big Data Industry Development Fund	30		**30**
China State-Owned Assets Venture Investment Fund	200		**200**
Guangdong Integrated Circuit Industrial Investment Fund		15	**15**
National Advanced Manufacturing Investment Fund	20		**20**
National Emerging Industry Investment Guidance Fund		40	**40**
National Small and Medium-size Enterprises Development Fund		15	**15**
Shenzhen State-owned Asset Reform and Development Fund		150	**150**
Xuzhou Industry Development Guidance Fund		40	**40**
Yangzhong Smart Yangtze River Guidance Fund		30	**30**
2016	**260**	**330**	**590**
Henan Industrial Agglomeration Area Development Investment Fund		60	**60**
Jiangxi Development Upgrade Guidance Fund		100	**100**
Shanghai Integrated Circuits Industry Investment Fund	50		**50**
State-owned Enterprises Guochuang Guidance Fund	150		**150**
Zhongyuan Silk Road Fund		20	**20**
Beijing Technology Innovation Fund		20	**20**
2017	**200**	**200**	**400**
Total	**884**	**1,090**	**1,974**

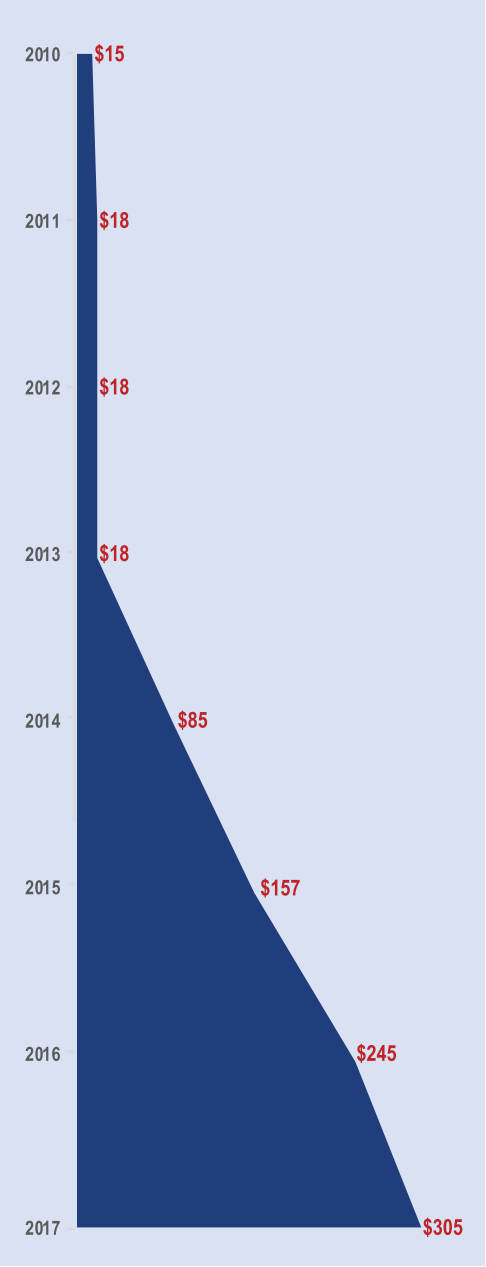


Table 2. Funds and funds-of-funds (not-exhaustive list) created by the Chinese Government to sustain innovation before and after Made in China began (billion ¥). Source: China Money Network, Barclays Research

The result of all these efforts and plans has been a continuous growth in research and in patent applications. Chinese acceleration push on patent application has been a radical change in the landscape of patent activity worldwide (Figure 5).

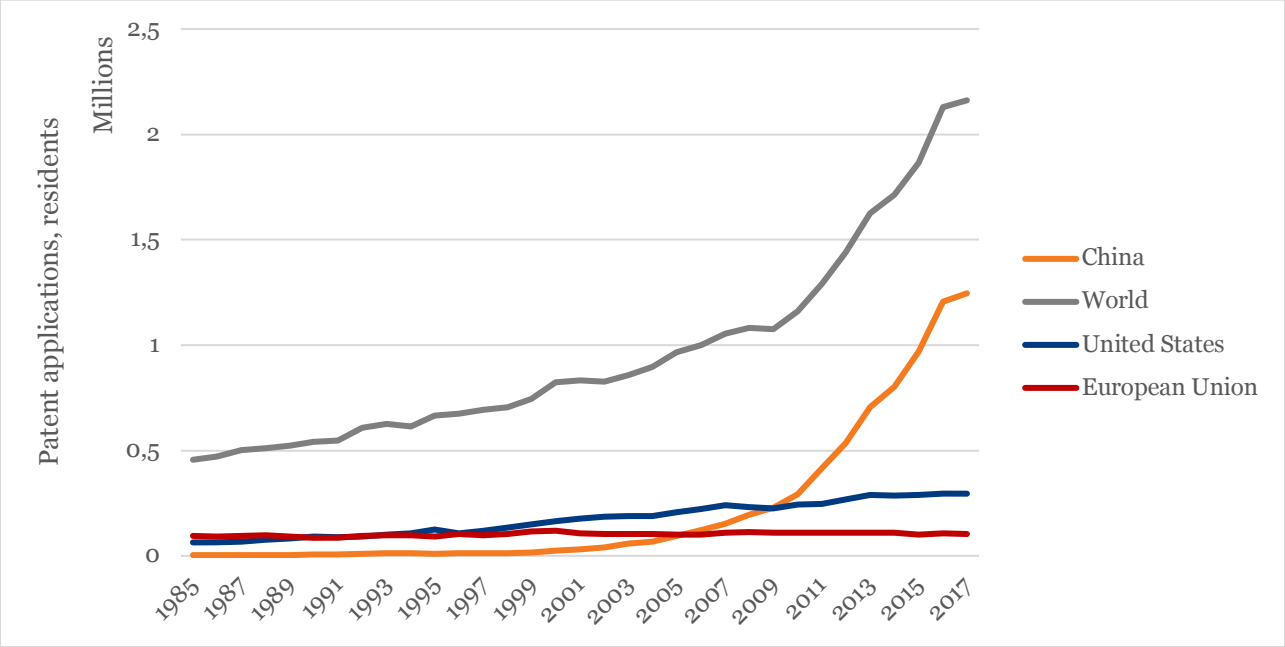


Figure 5. Patent applications of residents in the World, China, US, European Union (1985-2017, millions). Source: World Bank, 2019

Parallel to the increase of China's efforts in creating ever more truly Chinese products, the number of companies that protest alleged Intellectual Property theft has expanded. This is a core point of concern for the US administration in the ongoing trade dispute. These fears are heightened by China's recent Cyber Security Law, enacted by the Standing Committee of the National People's Congress on November 7, 2016 and implemented on June 1, 2017. The Law is an evolution of the previously existent cybersecurity rules and regulations from various levels and fields. It gives a systematic framework at the top of the pyramid-structured legislation on cybersecurity, including different topics surrounding its cyber security core. Among other things, the law provides that: foreign companies could be required to disclose some source code of their software and other IP to Chinese authorities; certain foreign companies have to store their information locally in China and, that is relevant for the future of 5G in Europe, Chinese companies have to cooperate with the State's efforts to collect cyber information.[38]

5.2. Huawei's role in global telecommunications

China excels in many industrial products, but the list of Chinese firms that have achieved sustained, large-scale international success based on technological leadership is not that long. Huawei involvement in trade litigation with the US is a serious problem for the Chinese government. It is the most frequently cited success story for the national challenge to transform the country into a competitive global leader in technology and innovation. It is a producer, not an assembler. Huawei is like a flagship of the most critical national challenge in an industry that matters worldwide and for a very sensitive political objective.

[38] Source: S. GUPTA, COLLINS B. et al. *5G Leadership: Huawei in Context*.

Huawei has been defined as the perfect example of a business model that is "80% of the quality for 60% of the price".[39] However, its strategy is evolving (Figure 5). Its focus is moving from B2B to B2C, demonstrating it can achieve leadership in both the markets. Up to 2018, the largest business in Huawei was the carriers' network. With growing international concerns about company security practices, this business had a halt. However, it did not stop the company's growth where the smartphone business, mainly a consumer-oriented production, was able to even increase its growth rate. The growth rate of its consumer business, mainly formed by smartphone with an increasing presence in the computer and tablet market (even in the US), has reached an astonishing average growth of 37% in 7 years. It is an impressive result in a hypercompetitive market, with a slowing growth and a replacement cycle that is getting longer and longer.

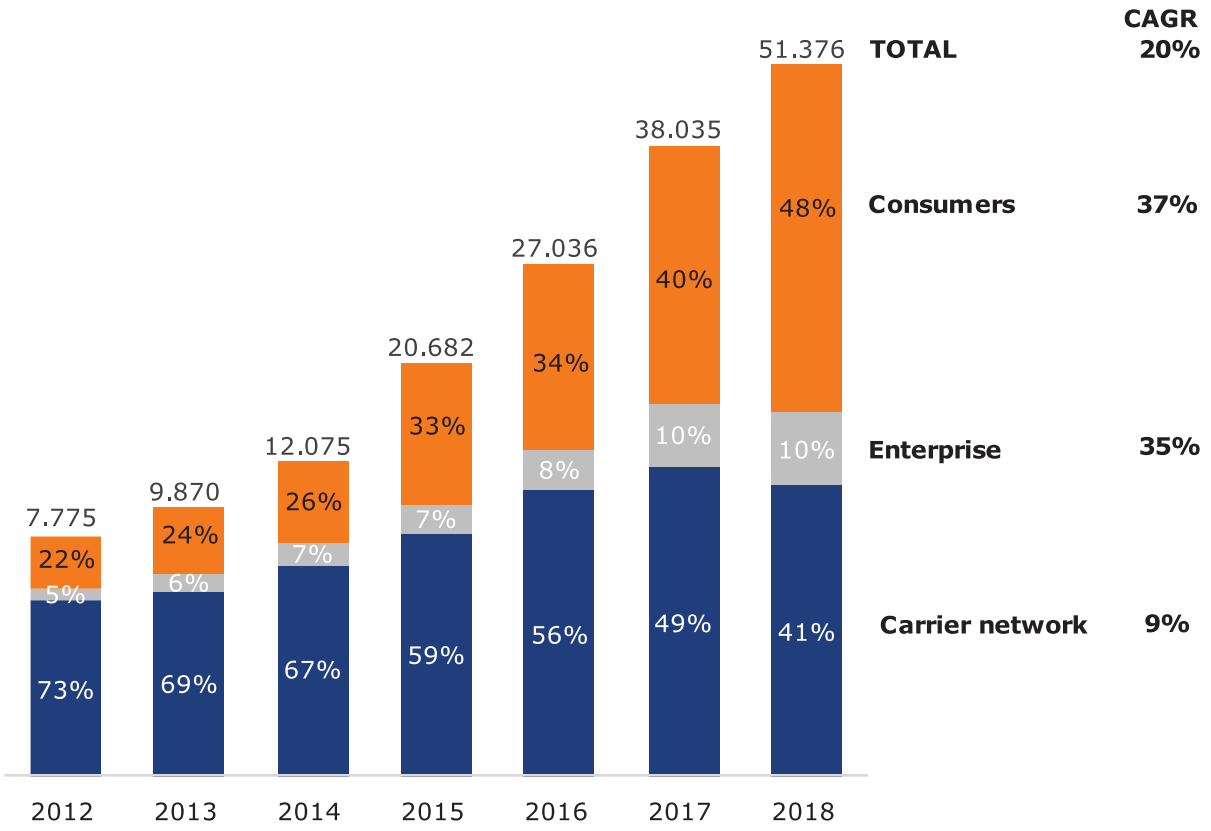


Figure 6. Huawei revenues by business segment (2012-2018, %, millions). Source: Company reports

Huawei's results prove being the global leader in the worldwide telecommunications equipment market can create synergies to exploit and transfer in adjacent markets. It happened in the enterprise networking business, doubled to 10% of company's revenues in seven years. Still, its most impressive and unprecedented achievement is in the consumer market. Both Ericsson and Nokia failed to reach or maintain leadership along the telecom value chain in the consumer business. Their challenges ended with an inglorious retreat, even if market conditions were much more favorable than today's, with an expanding market, at the beginning of the era of the smartphones. Contrary to what happened to Ericsson and Nokia, Huawei was able to reach a top player position in the consumer business and to improve it so much to overcome all the consequences of the Chinese-American trade war in the telecommunications equipment market (Figure 7). Despite the problems created by trade

[39] A. R. KROEBER *China's Economy*.

tensions with the US, Huawei's overall market share in the global telecommunications equipment sector – as well as for ZTE – went back to rise again in the first half of 2019. At the same time, Nokia and Ericsson started losing ground once more.

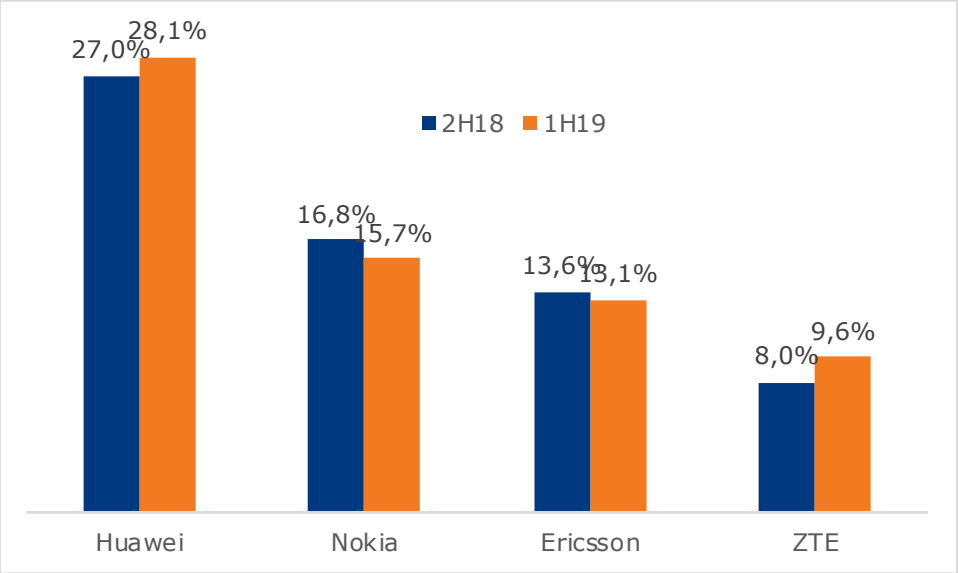


Figure 7. The global telecommunications equipment market: changes in market shares of market leaders between the H2 2018 and H1 2019. Source: Dell'Oro Group, August 2019

Huawei's leadership extends not only to the telecommunication industry but leads also in facial-recognition and other new surveillance technologies. It is well known that Chinese government use these tools at home. But Huawei Technologies Co. is exporting them globally, in Italy too, according to a new report by the Carnegie Endowment for International Peace. At least 75 countries around the world, from the US to Brazil, Germany, Italy, and Singapore, use AI to surveil citizens, the report said. China, selling to 63 countries, is the leading source of such technology (Japan is the second with 14 countries). Huawei, providing surveillance technology in 50 countries, is by far the leading company (Hikvision, another Chinese company, is the second with 16). Chinese product pitches are often accompanied by soft loans to encourage governments to purchase their equipment. These tactics are particularly relevant in countries like Kenya, Laos, Mongolia, Uganda, and Uzbekistan—which otherwise might not access this technology. This raises troubling questions about the extent to which the Chinese government is subsidizing the purchase of advanced repressive technology.[40]

Analyzed in detail, Huawei condition is unique in the telecommunication industry. In almost ten years it was able to reach a leadership position in every segment of the telecommunication industry, no matter if B2B or B2C, fixed or mobile (Figure 8). It is the first time that such a situation occurs in the history of telecommunications. No company has ever been even remotely close to a position like that of Huawei today.

[40] Source: S. FELDSTEIN (2019) *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, September, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf and R. TRACY (2019) «World Catching Up With China on Surveillance Tech», in *Wall Street Journal*, https://www.wsj.com/articles/world-catching-up-with-china-on-surveillance-tech-11568712601.

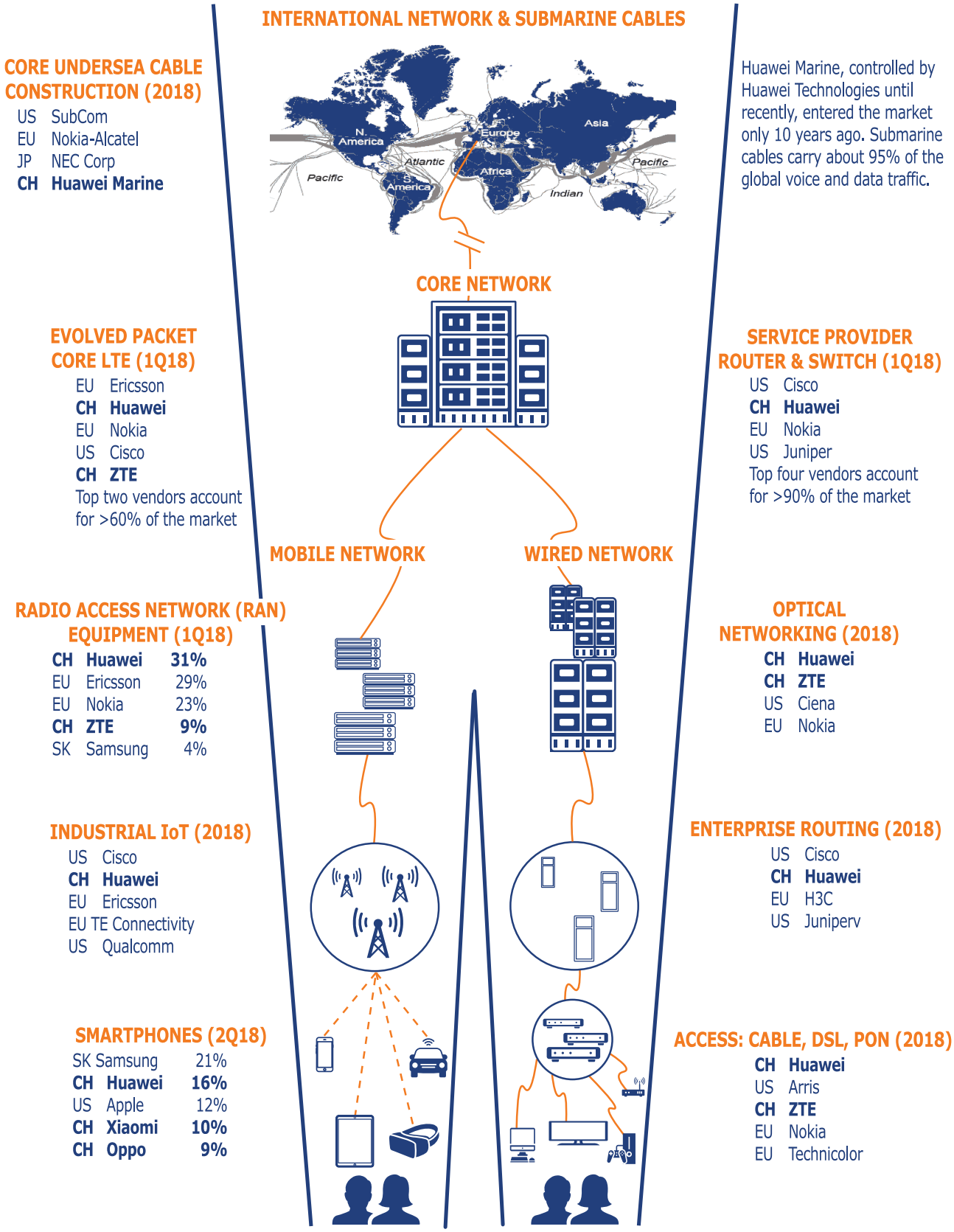


Figure 8. Leadership positions in the telecommunication business (mobile and wired) by business segment. Source: Dall'Oro Group, Statista, Business Insider Intelligence, Barclays Research

How did Huawei manage to reach this position? An example of its approach is what happened in the global Internet infrastructure equipment market. Once the decision was made to enter this market

and develop a set of products, Huawei initially concentrated its commercial effort in the more protected domestic market. With the volumes guaranteed by its internal market, while keeping prices significantly more competitive than the competition, it has continued to improve its products and then begin to focus its marketing effort on the most easily markets to target. Then, by gaining a more significant market share, he was able to finance new geographic expansions in relatively more challenging markets, further improving theirs products but also substantially weakening competition and so on, until it reached a leadership position.

In conclusion we see that Chinese operators are more integrated than others and, with specific regards to Huawei, we should note that they are:

- #2 players in mobile.
- #1 players in networks.
- #1 players in core systems.
- #4 players in submarine cables.

It is worth noting, at this point, that Huawei's business model doesn't support an open RAN and interoperability with other vendors and is not a member of the O-RAN.

Finally, UK's government has been running the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board jointly with Huawei for eight years to mitigate any perceived risks arising from the involvement of Huawei in parts of the critical national infrastructure. It should be noted that British officials said Huawei was slow to address problems identified in a previous review. In 2018, UK officials identified engineering shortfalls that they said led to discrepancies between Huawei software examined in the lab and software used in British networks. It found that Huawei's engineering processes couldn't re-create the same software from scratch twice—a key prerequisite for an adequate test of Huawei gear. UK officials said in their report[41] that Huawei didn't follow through on its 2012 pledges and as a result, they aren't confident about the company's recent promises to overhaul its cybersecurity practices. "Strongly worded commitments from Huawei in the past haven't brought about any discernible improvements," the report said. The report, written by the U.K.'s National Cyber Security Centre, is an annual update on a Huawei-run lab near Oxford, England, that examines the Chinese company's products used in British networks. It identified several specific, technical issues with Huawei's products and said the company has not fixed many of them. The lab in Britain, Huawei's oldest and most important major Western market, was the first to open. It employs Huawei employees, all British nationals with top-secret security clearance, and is overseen by board with officials from both the government and Huawei, as well as representatives from British carriers.[42]

5.3. News concerning telecommunication security issues and Huawei

- 2019: An article from the Wall Street Journal revealed WhatsApp and Skype communications of Bobi Wine, a pop star turned political opposition in Uganda, was spied by Huawei technicians on behalf of the Yoweri Museveni, the since 33-year President of Uganda. In the same article a second espionage case was reported. In Zambia, Huawei technicians helped the government access the phones and Facebook pages of a team of

[41] Source: HCSEC (2019) *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board - Annual Report 2019: A report to the National Security Adviser of the United Kingdom - March 2019*, HCSEC.

[42] Source: S. Woo (2019) «Huawei Equipment Has Major Security Flaws, U.K. Says», in *Wall Street Journal*, March 28, https://www.wsj.com/articles/u-k-says-huawei-gear-has-major-security-flaws-11553765403.

opposition bloggers running a pro-opposition news site, which had repeatedly criticized President Edgar Lungu. The two Huawei experts based in a cyber-surveillance unit in the offices of Zambia's telecom regulator pinpointed the bloggers' locations and were in constant contact with police units deployed to arrest them. The revelations focus attention on the surveillance systems Huawei sells governments, often branded "safe cities." The company has installed the systems in 700 cities spread across more than 100 countries and regions.

- 2019: the Dutch newspaper De Volkskrant published an article that said Chinese telecoms equipment maker Huawei had a hidden "backdoor" on the network of a major Dutch telecoms firm, making it possible to access customer data, citing unidentified intelligence sources.
- 2019: Huawei Technologies decided to sell its majority stake in Huawei Marine Systems Co. via cash and share issuance to Hengtong Optic-Electric Co., one of China's biggest makers of electric power and optical-fiber networks.
- 2019: According to a report by Finite State, a cybersecurity firm specialized in firmware security tests, telecommunications gear made by Huawei Technologies Co. is far more likely to contain flaws that could be leveraged by hackers for malicious use than equipment from rival companies after analyzing more than 1.5 million unique files embedded within nearly 10,000 firmware images supporting 558 products within Huawei's enterprise-networking product line.
- 2019: Poland arrested a Chinese Huawei executive and a former Polish security official on spying allegations. Recently, in a joint declaration with US, Poland stated suppliers of 5G network equipment should be rigorously evaluated for foreign government control.
- 2018: A planned Huawei Marine Networks submarine cable between Solomon Islands and Sydney canceled by the Australian government due to security fears.
- 2017: Australia's government blocked a deal for Huawei Marine to build a 2,500 miles cable connecting Sydney to the Solomon Islands, in the South Pacific, on the grounds that it created a cyber risk.
- 2012: Vodafone identified vulnerabilities with the Huawei-supplied broadband network gateways in Italy addressed the same year (see below - Bloomberg reported).
- 2011: Vodafone said it found vulnerabilities with the routers in Italy in 2011 and worked with Huawei to resolve the issues that year. In 2011, Bryan Littlefair, Vodafone's Chief Information Security Officer at the time reported in a classified internal report disclosed by Bloomberg in 2019: "What is of most concern here is that actions of Huawei in agreeing to remove the code, then trying to hide it, and now refusing to remove it as they need it to remain for 'quality' purposes," Littlefair wrote in 2012 (Bloomberg reported).
- 2009: Vodafone Said to Have Found Huawei Security Vulnerabilities since 2009 (Bloomberg reported).

6. THE KEY ISSUE

If in the past China was the factory of the world and the Western world was buying low tech items from them, like basic garments and toys, it is now a middle-income country and a technology powerhouse and it is proceeding fast in its intended development to become a global supplier of electric cars, smartphones, robots and AI systems. These are deep technologies that are embedded in our houses, infrastructures, communities and factories. These are all technologies that can be used with malicious purposes and that, once embedded in the systems, are hard and expensive to remove.

The key issue is that with 5G technologies, China can go deep into the Western world, which is a transparent democratic system, whilst China is a non-transparent communist system in which the State has given birth to companies in all the sectors of its interest and supports them with loans, investments funds and subsidies to the point that makes no sense to debate whether they are private or state owned companies. Further to this, the huge Chinese market is largely protected from the foreign competition and from it, Chinese companies make the revenues to compete globally.

Furthermore, Huawei has a line of credit of €88 billion[43] with the China Development Bank (CDB) that is owned by the Ministry of Finance and led by a cabinet Minister. According to EU standards, this open credit is an illegal subsidy that can enable Huawei to cut its prices in a way that competitors cannot. Huawei has grown from $4.6 billion of sales revenues in 2014 to $105 billion in 2018.

Since 5G will be also a struggle for supremacy, a country that wants to take appropriate measures to secure its 5G network, should consider the potential influence of the Chinese State on their vendors, both from the Chinese Communist Party (CCP) and from the Chinese Government, trying to implement its economic and industrial policy also using vendors as an extension of the State, financing them at non-competitive terms and having subjected them to the 2017 Chinese National Intelligence Law [44], a law that, different from other more standard security and spying legislations, is more active and states that:

"All organizations and citizens shall support, assist and cooperate with national intelligence efforts according to the Law."

In trading deep technologies "trust" is essential. Buying and selling technologies like 5G cannot be done without reciprocal trust. Total reciprocal business opportunity is key in this matter.

So important is the trustworthiness of the 5G network and so mission-critical are its applications that Mercedes-Benz has bought specific 5G private frequencies from the German government and is building a private 5G network with Deutsch Telefonica to implement intelligent manufacturing connecting all its factories.

6.1. The Technical issue:

From the technical point of view: 5G has an expanded surface of potential attack due to:

- The exposure of internal interfaces.
- The distributed architecture.
- The hyper-connectivity to IoT devices that have intrinsically low security posture.

6.2. The Policy issue

The Chinese policy framework does not protect the Chinese vendors - key players in 5G - **from undue influence from the State**: this represents a serious issue for Nation States willing to implement 5G.

[43] Source: https://henryjacksonsociety.org/wp-content/uploads/2019/05/HJS-Huawei-Report-A1.pdf

[44] Source: https://www.nytimes.com/2019/03/13/opinion/china-canada-huawei-spying-espionage-5g.html

6.3. The Economic issue

Another aspect to be considered is the reduced investment capacity of European telecom operators:

- **5G requires fiber densification** – To ensure backhauling connections to the thousands of new micro cells connected, there is a need for material investments, but telecom Operators are cash short and rely heavily on outsourcing, both for cost containment and lack of skills; they may be tempted by outside investments and in numerous cases they are already using Huawei equipment to save money and because they are the only ones ready for 5G.
- **European regulation resulted in lower prices and reduced investment capacity** – The European approach of "consumer first" has resulted in low-end user prices, but low returns for telecom operators. This is an obstacle to the investments needed for 5G, unless a non-economic element of ROI is included in the framework: how to do this within EU rules remains open and it most likely requires a change of approach that can only be European, developed and agreed with European Commission and its DGs, chiefly DG Competition.

Therefore, we have a situation where a revolutionary technology, potentially giving dominance to the winner, shows no clear business case yet: this can leave space for other types of play, not purely justified by an ROI logic. For example, Nation States, for whom achieving supremacy can be the key driver, or private players heavily supported by Nation States as seen for CDB support to Huawei.

The low returns of the European telecom operators, together with the leadership position of Huawei in most of the 5G supply chain, their competitive offers and high in-country investments, may lead some States to underestimate the broader security aspect. In an era where prosperity and security come from technology leadership developments, this is an issue.

It is also important to underline that a reduced cost for the deployment of 5G may come with a high cost for cyber-security measures to prevent attacks, which have a high cost themselves: ECIPE report estimates the cost of commercial espionage by State actors at $60 billion per year.

In risk assessment terms, both the probability of an incident and its potential impact are much greater in the 5G world compared to the current network setup: the potential impact of a security breach in the connected world of 5G is potentially disruptive. Threats may come from industrial espionage, military intelligence or political interference for hostile uses or in search of supremacy. FireEye reports 20 APTs – Advanced Security Threats attributable to a Nation State (Sept 2019), of which 11 are attributed to China, 3 to Iran, 2 to North Korea, 2 to Russian State and 2 to others (1 to Vietnam and 1 is not attributed).

7. THE OPPORTUNITY

The opportunity side lies in the investment and the value that 5G technologies will generate. Soon in Europe there will be very interesting opportunities to invest in the telecommunications infrastructure, but telecom operators have to find a way to sustain the investment cycle needed.

We have already quoted that investments needed for 5G in the next 15 years in Europe will be €500 billion and that there is an estimated shortage of €155 billion. At a global level, in the same period, 5G technologies will yield a GDP increase of $2,200 billion.[45]

The need for 5G to become a platform for Open Innovation is key point. In order to achieve this, the whole ecosystem with universities and startups should be allowed and encouraged to develop 5G

[45] Source: GSMA, 2019

open API interfaces, opening the whole 5G architecture: returning the Intellectual Property to those who developed the innovation and creating the opportunity to expand the transferrable skills.

8. SITUATION AND POLICY FRAMEWORK IN THE EU

8.1. Policy framework

The framework in which to operate is defined by the EU who recommended (March 26, 2019) a set of concrete actions to assess cybersecurity risks of 5G networks and to strengthen preventive measures.

The recommendations are a combination of legislative and policy instruments meant to protect EU economies, societies and democratic systems. At a national level, each Member State has completed a national risk assessment of 5G network infrastructures (July 19, 2019 - communication by Julian King, Commissioner for the Security Union, and Mariya Gabriel, Commissioner for the Digital Economy and Society.

These assessments will feed into the next phase: an EU-wide risk assessment where Member States should exchange information with each other and with the support of the Commission and the European Agency for Cybersecurity (ENISA), that will complete a coordinated risk assessment by October 1, 2019. On that basis, Member States will agree on a set of mitigating measures that can be used at national level.

National risk assessments therefore, will be a central element towards building a coordinated EU risk assessment.

EU Member States have the right to exclude companies from their markets for national security reasons if they do not comply with the country's standards and legal framework. Until now, though, no Member State has implemented and ban on Chinese company, unlike others in the world: countries that have banned Huawei make up nearly a third of the world's GDP.[46]

Some EU countries are already adapting their law to cater for the new challenge given by the 5G. The principle is that, because 5G changes the perimeter of the core network, governments are deploying or studying ways to extend their control to the new, enlarged, perimeter; i.e. Governments want to be able to ban materials suppliers to private operators if they come from outside EU vendors that are deemed to represent a threat to national security. In France this takes the form of the "Bothorel Law", in Italy it is the enlarged scope of the "Golden Power". Bothorel Law extends the technical security assessments by the French cyber agency, ANSSI and gives the PM office's power to exclude vendors if necessary. Italy's Golden Power law, being relaunched in these days (September 17th, 2019) and now a matter of urgency for the new Government:

- Defines the national perimeter of cybersecurity, including all actors involved in essential services and all activities based on telecom networks and IT systems that, in case of failure, would impact on national security.
- These actors will be subject to report any security issue and to disclose their procurement of goods and services to government for possible ban.

[46] Source: International Monetary Fund GDP data for 2018; Bloomberg

8.2. New regulation

As at the beginning of this document, the profitability of telecom operators in Europe is low, and even lower in Italy. There is now a new EU's telecom regulatory framework that promotes co-investments and sustainable competition. This must be approved by Member States before December 31, 2020. Meantime in Italy, Vodafone and Telecom have officially established a partnership to co-develop their 5G network.

The Union has also adopted an instrument that will protect critical infrastructure and technologies, such as those used in communications, by allowing Member States to screen foreign direct investments on grounds of security or public order and by creating a cooperation mechanism where Member States and the Commission will be able to exchange information and raise concerns related to specific investments.[47]

8.3. Conclusions

The aim of the new laws and regulation is to defend Europe's sovereignty in the context of a commercial war between US and China with its uncertain outcome.

European countries are struggling between security and geopolitical issues, tempted to avoid Chinese vendors for security reasons and, at the same time, trying not to be too dependent on USA. Abroad, Europe's access to important markets is increasingly limited on security ground: both USA and China are limiting untrusted foreign vendors in their networks on security grounds and Europe is the only one who doesn't. At Home, Europe is affected by cyber espionage, against which it lacks, for now, a common holistic approach: diplomatic, strategic and technological.

Laws, like the French "Bothorel" and the Italian "Golden Power", would give a tool of last resort to Governments, but are not silver bullet for security: addressing the 5G security issue requires more specific preventative actions to be deployed, including ethical considerations. In other words, do Europe and China really have the same democratic values and approach to fundamental rights? (see for example the UK debate).

Unlike Western analysts, where we find a fatal contradiction between a dynamic economy and a tightly controlled political structure, Chinese leaders see the two as complementary. Tight political control provides the stability within which economic activity can be decentralized; and the resulting rapid economic growth in turn enhances the party's legitimacy for having "delivered the goods" of higher living standards. With strengthened legitimacy, the party's grip on power becomes more secure, and most of people find the risk of switching to another, untried system to be unacceptably high. The ideas that economic growth is the key to sustained political power and that a government's legitimacy can just as well spring from economic growth as from democratic elections, are not uniquely Chinese creations. They are also common in China's successful East Asian neighbors, whose experiences Chinese leaders have studied closely since the beginning of the reform era.

9. CONCLUSIONS AND RECOMMENDATIONS FOR ITALY WITHIN EUROPE

In conclusion of the analysis, there are 3 key messages that we want to convey on the issue and the opportunity of the 5G security:

[47] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union OJ L 79l, 21.03.2019, p.1-14.

1. **There is a new level of security risk** – 5G has a significant increase in the vectors of attack and risk of greater negative impact for the economy and society if the attacks are successful.
2. **The geopolitical aspect of the risk is crucial** – The legal frameworks in non EU countries do not always grant that States cannot exert undue influences on vendor companies.
3. **A country can grow its GDP by addressing the 5G security issue** – Becoming an inherently trustworthy ecosystem would create a better business environment and foster investments. Not doing it, can have significant costs in terms of industrial espionage and systems' disruption.

Working as single entities will not yield results: Only a Single Market approach can give to Europe the needed gravitas in the negotiations with the US and China.

The first reaction of a country can be one of closure, but this would bring to a slowdown of economic growth. Also, the interdependency that exists between private companies and States, amongst States and amongst companies in different States, is a further factor to be considered: on one level, States aspire to national supremacy and, in this era, this implies having a leading edge in technology. On another level, international co-operations and partnerships to develop new technologies are thriving and the supply chains of many sectors, including 4G and 5G, are interconnected. This paradox shall be considered when addressing the 5G issue.

We believe that the approach should be holistic: technology, geopolitical strategy, policy are all key aspects of the matter; Europe should act as a single entity and have one approach.

9.1. Objective: to build an inherently trustworthy infrastructure in Italy

Building an inherently trustworthy 5G infrastructure would make Italy a more attractive place for investments.

An inherently trustworthy infrastructure implies a low level of risk even when things go wrong. In risk assessment terms, it means to minimize the probability that a negative event happens and/or to minimize the impact of such an event.

To achieve this inherent security, one should act in the design phase of the system, from the selection of the vendors, auditing the bulk of their processes in order to reduce the probability that a negative event materializes; to giving critical applications systems a level of redundancy, in order to reduce the impact of negative events when they happen: to achieve this, it is necessary to carry out an assessment of the critical infrastructures.

There are 2 different aspects to trustworthiness: policy and technical.

9.2. Policy aspects

The key point here is to analyze the governance system of the vendors outside EU and the legal framework of their State by assessing the vendor and the government to whom they might be beholden.

Vendors should have, and show evidence of, a strong governance system and explain how they would manage influence that may be exerted by an external party or State authorities[48] trying to obtain an undue advantage.

For vendors, the analysis should specifically address the following points:

- The ownership structure and its transparency.
- Any other additional ties to the state and the likelihood of undue influence.
- Their business model and interoperability with other vendors.
- The impact of the US entity list and whether this undermines their quality, sustainability and security.

And last, but not least:

- An analysis of their past behavior and their security track record.

For Governments, the analysis should address:

- Their offensive cyber practices – both in terms of the legitimacy of the target and whether they are directed towards Italy/EU.
- The legal framework in the country as it relates to cooperation with intelligence agencies.
- The rule of law and alignment of values of the country.
- The fairness of their economic support for vendors.
- The reciprocity of their own approach to security and market access for European vendors.

In case of non-satisfactory compliance, the telecom operator may decide not to opt for that vendor.

If it does however, the EU Member State can appeal to the EU framework on the "Screening of Foreign Direct Investments" and on the "Golden Power" that the Italian State has extended to 5G network for non-European vendors.[49]

9.3. Technical aspects

The most important technical aspect refers to the vendors' supply chain audit, which should include:

- Assessing the security of the development lifecycle – Aimed at proving trustworthy approach in designing and developing software and hardware.
- Assessing the measures to mitigate supply chain risks – Including counterfeit components and malicious insertion of third-party alien components.
- Assessing Software Authenticity and Integrity – Software is not modified un-intentionally or intentionally, creating security vulnerabilities and backdoors.
- Assessing the presence of trust anchor modules in each critical product – e.g. certificates, secure storage etc.

[48] States are immune to prosecution before foreign courts: The United Nations Convention on Jurisdictional Immunities of States and Their Property was adopted by the General Assembly on 2 December 2004 but is yet to come into force.

[49] In Italy, Legge 25 marzo 2019, N 22, The new law extends State's veto power beyond share purchase, to the sale of services and products in strategic sectors – currently it seems to be on-hold

9.4. Recommendations for Italy

Within the broader contexts depicted above, we specifically recommend to Italian Policy Makers (PM) and Industry Players (IP) to deploy the following 3 measures, with the key objective to create an Italian 5G system that is inherently trustworthy:

1. **An assessment of its critical infrastructures** (1, 2, 3 priority level) – PM, IP
2. **A process to audit the whole supply chain of the vendors** (see above) – PM, IP
3. **The establishment of a COE - Centre of Expertise for threat intelligence** – PM, IP, where processes and experiences are continuously shared with like-minded countries and bring to augmented capability where threats are:
   - Detected faster
   - Contained faster
   - Fixed faster

The Centre Of Expertise for threat intelligence would offer a unique give and take approach: contribute to global cyber threat intelligence the Italian visibility of network behavior and symptoms of cyber-attacks and receive, in exchange, real time updated global view that allows to anticipate attacks but it's also very relevant to the local Security reality in Italy. It would favor collective learning and would result in augmented capabilities for all cybersecurity aspects. It would also contribute to creating new employment and new competencies that can spill over to the industrial sector, in an open innovation logic, support the digital transformation and foster the economic development of the country.

In case of vendors who are definitely rated as untrustworthy, Italy can adopt a series of bans: from exclusion tout court, to exclusion from core network, to bans on specific products, locations, customers, but this would be a last resort type of approach (made possible by the extension of the "Golden Power", if confirmed), whereas a more sensible one is to follow the recommendations outlined above and require the application of certain non-negotiable principles.

At country level, the implementation of an **Italian 5G system** that is **inherently trustworthy** would **increase the attractiveness of the country** for foreign investors, who have increasing concerns on how to protect their intellectual property and create a favorable business environment. For SMEs, the backbone of Italian economic system, who that needs to undergo the digital transformation if they want to survive.

9.5. Final remarks

Finally, and most importantly, when looking at 5G security it is extremely important to take a holistic approach, there are two points to be considered when looking at 5G security in a broader way.

The first is that the 5G security is not purely related to cybersecurity issue: geo-economy shall be considered as an integral part of it, given the role that 5G plays in the increasing economic competition between Nation States and economic blocks, especially between US and China.

Secondly, cyber risks are defined in a very technical way, looking at cyberattacks and backdoors, while the correct approach would be to look at the evolution of our digital world and how social networks can influence the public opinion.

In a report on 5G and the 5 Eyes Alliance written for the Henry Jackson Society by Seely, Varnish and Hemmings, they state that:

"While the Government might believe that an unquantifiable but potentially significant amount of political and security damage is worth the exchange for the promise of economic and investment gains, there are two flaws with this argument. First, it does not really weigh in the wider geopolitical trend that sees the US and China moving toward greater strategic and economic competition. (.....) (UK) might find itself losing influence at an ever-increasing rate with a country that – while imperfect – remains a democracy with similar values and norms to the UK.

Second, it identifies technical risk in the narrowest of ways – looking for backdoors and cyber-attacks – and completely misses the emergence of two worrying trends: first, the development of social media, Big Data, and Artificial Intelligence being used to harvest immense amounts of data on societies. Second, the interest and growing expertise of authoritarian powers in the application of these technologies in controlling and influencing populations. The narrow band of risk assessment and mitigation that only considers about data breaches or system failure but ignores the slow build-up of data about the UK's military leaders, its political leaders, and its media influencers and owners, betrays an unsophisticated understanding of technological risk. It is to all intentions and purposes – risk so narrowly defined as to be useless."

REFERENCES

Balding, C. And Others (2019) *Who owns Huawei*, Henry Jackson Society, https://henryjacksonsociety.org/members-content/who-owns-huawei/.

Bhunia S., Hsiao M. S., Banga M. et al. (2014) «Hardware Trojan attacks: threat analysis and countermeasures», in *Proceedings of the IEEE*, 102, 8, pp. 1229-1247.

Cimpanu C. (2019) «Germany: Backdoor found in four smartphone models; 20,000 users infected», in, June 6, https://www.zdnet.com/article/germany-backdoor-found-in-four-smartphone-models-20000-users-infected/.

Domas C. (2018) «Hardware Backdoors in x86 CPUs», in, Black Hat, July 27, https://i.blackhat.com/us-18/Thu-August-9/us-18-Domas-God-Mode-Unlocked-Hardware-Backdoors-In-x86-CPUs-wp.pdf.

Feldstein S. (2019) *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, September, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

Finite State (2019) *Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd.*, Finite State, https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf.

Friedman T. L. (2019) «How Trump and Xi Can Make America and China Poor Again», in *New York Times*, August 6.

Gsma (2019) *Modernise regulation to deliver Europe's digital future calls GSMA*, GSMA, February 26, https://www.gsma.com/newsroom/press-release/modernise-regulation-to-deliver-europes-digital-future-calls-gsma/.

Gupta S., Collins B., Rekrut D. et al. (2019) *5G Leadership: Huawei in Context*, Barclays Research, 5 June.

Harbor Research (2018) *The Private LTE Opportunity for Industrial and Commercial IoT*, Harbour Research, https://www.multefire.org/wp-content/uploads/HRI_Paper_Private-LTE-Network-Paper_20-July-2017_Final.pdf.

Hcsec (2019) *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board - Annual Report 2019: A report to the National Security Adviser of the United Kingdom - March 2019*, HCSEC.

Kirk J. (2013) «D-Link issues fixes for firmware backdoor in routers | Computerworld», in *ComputerWorld*, December 3, 2013-12-03T05:51-05:00.

Kroeber A. R. (2016) *China's Economy*, New York, Oxford University Press.

Lepido D. (2019) «Vodafone Found Hidden Backdoors in Huawei Equipment», in *Bloomberg*, April 30, 2019-04-30T06:45:12.877Z.

Li L. (2018) «China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0"», in *Technological Forecasting and Social Change*, 135, 2018/10/01/, pp. 66-74.

Liyanage M., Ahmad I., Bux Abro A. et al., Eds. (2018) *A Comprehensive Guide to 5G Security*, Hoboken, NJ, John Wiley & Sons.

Perlroth N. (2014) «Russian Hackers Targeting Oil and Gas Companies», in *New York Times*, June 30, https://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html?searchResultPosition=1.

Strumpf D. and Cherney M. (2018) «Australia's Actions Against Chinese Firms Ignite 5G Security Debate», in *Wall Street Journal*, September 12.

The State Council of the People's Republic of China (2006a) «China issues science and technology development guidelines», in *Gov.cn*, February 9, http://www.gov.cn/english/2006-02/09/content_183426.htm.

--- (2006b) «The National Medium- and Long-Term Program for Science and Technology Development (2006-2020) - An Outline», in *Gov.cn*, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf.

--- (2017) «Building a world manufacturing power — Premier and 'Made in China 2025' strategy», in *Gov.cn*, January 31, http://english.www.gov.cn/premier/news/2017/01/29/content_281475554068056.htm.

Tracy R. (2019) «World Catching Up With China on Surveillance Tech», in *Wall Street Journal*, https://www.wsj.com/articles/world-catching-up-with-china-on-surveillance-tech-11568712601.

Vashistha N., Lu H., Shi Q. et al. (2018) *Trojan Scanner Detecting Hardware Trojans with Rapid SEM Imaging Combined with Image Processing and Machine Learning*.

Woo S. (2019) «Huawei Equipment Has Major Security Flaws, U.K. Says», in *Wall Street Journal*, March 28.

Xiao K., Forte D., Jin Y. et al. (2016) «Hardware trojans: Lessons learned after one decade of research», in *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 22, 1, p. 6.

Yang K., Hicks M., Dong Q. et al. (2016) *A2: Analog malicious hardware*, 2016 IEEE symposium on security and privacy (SP), IEEE.

Zetter K. (2019) «Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers», in *Vice*, March 25, 2019-03-25.

Nome file: 191104_Ambrosetti_5G.docx
Directory: /Users/andreasoldo/Library/Containers/com.microsoft.Word/Data/Documents
Modello: /Users/andreasoldo/Library/Group Containers/UBF8T346G9.Office/User Content.localized/Templates.localized/Normal.dotm
Titolo:
Oggetto:
Autore: andrea soldo
Parole chiave:
Commenti:
Data creazione: 05/11/19 10:17:00
Numero revisione: 1
Data ultimo salvataggio: 05/11/19 10:17:00
Autore ultimo salvataggio:
Tempo totale modifica 0 minuti
Data ultima stampa:
Come da ultima stampa completa
Numero pagine: 35
Numero parole: 19.499 (circa)
Numero caratteri: 111.148 (circa)