BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

THE HIDDEN COST OF UNTRUSTED VENDORS IN 5G NETWORKS

State Of Discussion And Estimations For France

Reda YAICH, Philippe LAURIER
December 2020

Contact and further information :

Brandenburg Institut for Society and Security gGmbH (BIGS)
Managing Director: Dr. Tim H. Stuchtey
Dianastrasse 46
14482 Potsdam
Phone: +49-331-704406-0
Fax: +49-331-704406-19
E-mail: direktor@bigs-potsdam.org
www.bigs-potsdam.org

This country study is an addendum for France of the BIGS Policy paper “The Hidden Cost of Untrusted Vendors in 5G Networks”. The study was commissioned by BIGS and conducted by IRT SystemX.

IRT SystemX
Centre d’intégration Nano-INNOV
Bât N3 –8, Avenue de la Vauve
CS 90070, 91127 Palaiseau Cedex
contact@irt-systemx.fr | www.irt-systemx.fr

This study was funded by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the authors and do not necessarily reflect those of the United States Department of State.

Table of Contents

Accronyms

Abbreviations	Meaning
ANSSI	National Cybersecurity Agency of France (Agence nationale pour la sécurité des systèmes d'information), in charge of networks security. It depends on the Prime Minister's General secretariat of defense and national security (SGDSN).
ARCEP	Electronic Communications and Postal Regulatory Authority (Autorité de Régulation des Communications Electroniques et des Postes) in charge of competition regulation.
ANFR	National Agency of Frequencies (Agence nationale des fréquences) is an administrative authority in charge in particular of the management and allocation of 5G frequencies. It also controls the use of these frequencies.
OIV	Operator of Vital Importance
OSE	Operator of Essential Services
LPM	French Military Programming Law, obliging operators of vital importance (OIV) to adopt specific security measures
NIS	Network and Information Security
SFR	Société Française du Radiotéléphone

A- INTRODUCTION

In July 2019, the French government adopted a roadmap to accelerate the deployment of 5G networks, coordinated by the work program of the Electronic Communications and Postal Regulatory Authority (ARCEP). The key milestones of this roadmap include: (1) launching 5G pilots in different regions and settings, (2) freeing up and allocating new frequencies, (3) preparing for the effective deployment of 5G in at least one city in 2020 and covering the main transport axis by 2025, (4) encouraging the development of new industrial uses, and (5) ensuring transparency and dialogue around the deployment of 5G and public exposure.

In addition to the aforementioned key milestones, the government explicitly identified "cybersecurity" as a key challenge that will necessarily call for additional requirements and new regulations in which the National Cybersecurity Agency of France (ANSSI) will play a central role. Guillaume Poupard, ANSSI director, declared that "5G networks will be as sensitive and critical as power grids". Among the potential risks, the government listed "espionage", "subversion of information processes" and "network dysfunctioning" as the most significant (this study will later examine and quantify the risk of cyberattack).

In this context, the French government adopted in 2019 and 2020 a series of measures to regulate the activity of 5G equipment manufacturers prior to the first rollout of 5G networks in France. In an interview[1], ANSSI director claimed that the "Operators who don't use Huawei are encouraged to avoid it because it's the natural sense of things … we're just saying that the risk is not the same with European equipment manufacturers as with non-Europeans. We must not lie to each other".

Along with ANSSI, the French mobile telecom market is regulated by an independent administrative authority: Arcep (Autorité de Régulation des Communications Electroniques et des Postes), whose mission is to support the opening up of the telecommunications sector to competition, and to ensure that competition between operators is fair and serves the benefit of consumers.

Overall, three state bodies play a direct role :

- **ARCEP** is responsible the competition regulation of the market and operators competition.
- **ANSSI**, National Cybersecurity Agency of France, is the main decision-maker when it comes to the security-related aspects of 5G. It is responsible for providing accreditation to suppliers and authorising or prohibiting the use of specific network equipment.
- **ANFR** is the National Agency of Frequencies. It is the main actor in charge of the management of 5G frequencies. It decides if a specific site (including the base station and its antennae) is authorised to operate. It is also in charge of monitoring the compliance of operators and equipment with frequencies usage rules and policies.

As a first step, 5G will mainly reuse 4G sites. In November 2020, there were almost 49,000 active 4G sites for all operators (some mobile phone base stations have several antennae. Conversely, some sites are pooled for several operators). 54,000 sites are already authorised, compared with 38,500 in January 2018.[2] The Free network is under construction. This means that 4G deployment is not yet fully achieved in France.

1- https://fr.reuters.com/article/idfrkbn2470eh-ofrin
2-https://www.anfr.fr/fr/toutes-les-actualites/actualites/observatoire-anfr-pres-de-54-000-sites-4g-autorises-par-lanfr-en-france-au-1er-septembre/

French Operator	Number of sites (Nov. 2019)
Orange	20,646 sites
SFR	18,218 sites
Bouygues Télécom	17,729 sites
Free Mobile	14,205 sites

Due to the technical need to densify the network of antennae, some evaluations expect the number of antennae to increase by 30% (from 4G to 5G) during the transition between 4G and 5G. This means the number of antennae will grow to 100,000 for 5G.

B-STATE OF AFFAIRS

B.1 CURRENT DEBATE IN FRANCE

The debate around the presence and the possible danger posed by Huawei in France is already longstanding, dating back to the 3G period. This certainly contributed to containing Huawei's entry into the French telecommunications market, where the company's presence is currently lower than in the majority of other European countries. Some of the first warnings against increased Huawei operations in France came from state security services (concerning a possible risk of tapping communications[3]), and on the other hand from trade unions. In 2017, before a parliamentary commission of inquiry[4], trade unions reiterated their accusations that "Huawei used all possible means to gain competence and gain market share" (Olivier Marcé – CFE CGC trade-union) and more precisely that "Huawei practices very low prices because they are subsidized. (…) It practices an extravagant dumping, in China, but also and mainly in Europe, where we are being pushed out of the market" (Pascal Guihéneuf – Cfdt Trade Union). The accusation also addressed European leniency, which has led it to accept "the technology transfers which have greatly helped Huawei and ZTE to develop until now and surpass us" (Claude Josserand - CGT Trade Union).

Answering a question from the rapporteur of the commission (Guillaume Kasbarian, MP) about effective means of containing this rise in power, one of their proposals stated "one can wonder about the accounts of this company. We ignore them. Could it not be imagined that some markets would be reserved only to companies that publish their accounts ?"

> It should be pointed out that this transparency axis reminds underutilised, in particular with regard to accounting transparency, with greater emphasis placed on technological transparency.

One of these witnesses has since reiterated his accusations in a newspaper (L'Humanité), reporting that SFR deployed in October 2018 the first 5G antennae manufactured by Huawei on the roof of its Parisian headquarters, only tens of metres from the Ministry of Defence HQ. However, in something of a gentleman's agreement, Paris was previously tacitly listed as a high-security zone that would preferably be free of any suppliers about which uncertainties remained. This red line crossing triggered the 2019 law, discussed below, which formalises these previously tacit geographical restrictions.

In terms of 5G deployment, France promulgated a new law[5] in August 2019 to "restrict or prohibit or impose requirements or conditions" for the supply, deployment and operation of 5G equipment. The law obliges telecom operators and 5G vendors to receive specific authorisation from ANSSI, which depends on the prime minister's office, before rolling-out and operating sensitive equipment for 5G (and future technology, such as 6G) networks. For an operator to obtain authorisation, all technical and operational information must be provided to ANSSI, as well as the list of contractors involved.

3- One can also refer to the following Rapport d'information: "La cyberdéfense: un enjeu mondial, une priorité nationale" written by Senator Jean-Marie Bockel on this subject in 2012: https://www.senat.fr/rap/r11-681/r11-6811.pdf

4-« Commission d'enquête sur les décisions de l'Etat en matière de politique industrielle ». 2017.

5-« Law aiming to protect the interests of the national defense and national security about the operation of mobile radio networks » (n° 2019-810. « Loi du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles »). Rapporteur Eric Bothorel mp. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038864094

B.2 THE INDUSTRIAL AND SOCIAL SIDE, AND THE LOBBYING WORK OF THE STAKEHOLDERS

The attitude and criticisms of the trade unions can be explained by their concerns about the impact on employment in the French telecommunication production plants. This social and industrial perspective plays a significant part in the ongoing debates. It is taken into account in the strategies of all suppliers interested in the French market. In January 2020, Ericsson opened its first research centre in France, near Paris, which will employ 300 people in the future. The company announced that this new plant will be specialised in 5G software and 5G security. Conversely, in the same year, Nokia announced a workforce reduction plan that will affect 1,200 employees in its French research plants.

On its side, Huawei has taken several initiatives :

◆ In October 2020, Huawei opened a research centre in Paris. Its areas of interest will be mathemathics, computer calculation and artificial intelligence. It is the sixth of its kind in France, and intends to initially employ 30 researchers. The previous centre was opened in 2018 near the town of Grenoble, and was expected to employ 30 people in 2020. The others are located in Boulogne-Billancourt (two plants), Paris and Sophia-Antipolis. Altogether, these research and design centres employ about 200 people. Ms Valerie Pecresse, president of the Paris region, declared recently: " Once again, I would like to congratulate Huawei for this choice, which reflects the quality of our research. " At the time of the inauguration of the previous Huawei plant in Paris, a government representative and a member of the Paris city council in charge of innovation, research and universities attended the event. These facts underscore the existence of local efforts by Huawei to create close relationships with the political sphere.

◆ In November 2020, Huawei announced plans to open a factory specialised in the production of 5G equipment, near the town of Strasbourg. According to various sources, this EUR 200 million investment has the objective of recruiting 300 employees, and 500 in the future. Once again, Huawei's relational work has made it possible for the company to gain the support of regional authorities, of the metropolitan area authorities, and of the chamber of commerce. The president of the region Jean Rottner declared that " we've been working on this file with Huawei for months now ", adding that he was " pleased to salute the leaders of Huawei " for " this excellent news ". Press comments wrote that " With the promise of hundreds of new jobs, Huawei could hope to attract the sympathy of the government ".[6] In response, the current Minister of Economy Bruno le Maire declared in April 2020 that "we simply look after our security and strategic interests (and) the decisions of the State will not be changed", but that he employs no discriminatory practice to the detriment of any telecommunications equipment supplier.

The above elements indicate that the opening and closing of industrial or research plants have become factors likely to influence the views of the French authorities, to strengthen links with the political sphere, and to influence the general public's opinion.

This outreach tactic, common as it may be in sensitive industries such as telecommunications, is characterised by its recurrence at each Huawei inauguration. Already in 2015 and 2016, at the time of the announcement of the creation of research centres in Paris, two government ministers attended the ceremonies. The press reported that " this (Huawei) seduction offensive is perhaps in response to a draft legislation aiming to make mandatory the certification of any telecommunication system, in the name of national security "[6]. Such a law was finally passed in 2019 (see above, law n° 2019-810).

In response to this strategy, some elected officials or association leaders have voiced criticisms about the arrival of 5G production facilities – for environmental or health reasons – and occasionally more directly against Huawei. For example, Stephen Kerckhove, general delegate of the association Acting for the environment (Agir pour l'environnement), stated: " About the issue of cybersecurity, authorizing Huawei to produce in France 5G antennae components is becoming an

6- Romain Pomian-Bonnemaison : « 5G : la construction d'une usine Huawei en Alsace n'adoucira pas la position de la France ». Magazine Phonandroid, 04/03/2020.
7- « Huawei veut créer 170 emplois en France dans la R et D ». Magazine Entreprendre, 03/11/2014.

accomplice of the collection of personal data, on a scale to the power of 100 in comparison with 4G technology. Do we want a society where 5G will enable multinational companies such as Huawei to spy on us in our every move and in our slightest actions ? ”[8]

8- In Martin Antoine: « Strasbourg: la création d’une usine d’antennes 5G Huawei divise les élus ». Le Parisien libéré, 10/10/2021.

B.3 TELECOM PROVIDERS

The mobile telephone market is contested by four MNOs, and some MVNOs. The main one is Orange with one third of the market, followed by SFR with one fourth of the market, followed by Free and Bouygues, which each hold about one fifth of the market.

Orange (spring 2020)	19.388 million subscribers (to which should be added 2,207 million that have prepaid cards)
SFR (spring 2020)	14.479 million (and 1.4 million with prepaid cards)
Free (spring 2020)	13.326 million
Bouygues Telecom (spring 2020)	11.7 million (since Bouygues bought 5 MVNOs in the summer of 2020, which added 2 million new clients)
Total	58.893 million

◆ The number of people who have a mobile phone is 65 million, 99% of the population.
◆ The mobile phone equipment rate of the population is > 100 % since 2011, but is now growing more slowly, and has reached 106.2% (2017).
◆ Number of SIM cards without MtoM = 77 million (2019[9])
Number of SIM cards with MtoM = 19.2 million (2019), rising quickly
- 77 + 19.2 = 96.2 millions of SIM cards in France.

◆ EUR 12 is the average price of a mobile phone package in France in 2019 (incl. tax per month). By comparison, for the same package, Germans pay EUR 45 and Spanish EUR 40. France has the lowest rates in Europe [French Association of Telecommunications].
◆ The average mobile connection speed was 17.4 Mbps (megabytes per second) in France in 2016, compared to 10.7 in the United States and 9.3 in China.

In the broadband and ultra-broadband market, the French telecom market was, at the end of 2019, dominated by Orange, by far the leading operator.

Orange	41.6% market share	12.35 million subscibers
FREE	22.2%	6.46 million subscibers
SFR	21.9%	6.36 million subscibers
Bouygues Telecom	13.4%	3.9 million subscibers

9- https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/observatoire-services-mobiles/abonnes-mobiles-t3-2020.html

B.4 THE MOBILE TELECOMMUNICATIONS CORPORATE MARKET

Regarding the risks to economic or state activities, the corporate market is the key sector, together with the regalian and public sector (the army and police as well as administrations, universities, and research centres). The size of the corporate market is nevertheless small in comparison with the global telecommunications market.

The market global turnover - fixed and mobile telecommunications- was EUR 30.677 billion in 2019

in which EUR 13.316 billion relate to mobile communications

in which 18% relate to business clients (EUR 2.3 billion)

This small size must be compared with the size of the fixed telephony – also small – and their respective use by companies. Such a comparison underlines the growing dependence of companies on mobile telecommunications.

In 2017, the number of subscriptions with companies to mobile telephony has surpassed the subscriptions to fixed telephony.	At the end of 2018, the mobile phone market's number of subscriptions amounted to 9.0 million, with growth of about 3% per year; the fixed telephone market, in steady decline, amounted to 8.4 million.
In traffic volume for companies, the switchover occurred in 2016.	19.5 billion minutes with mobile phones; 16.6 for fixed phones (2018).
	This move to the first row, which is a handover, underlines the strategic importance of mobile phone equipment for the business world. This strategic nature is reinforced by the average monthly volume of companies' data transmitted by mobile phone, growing strongly (1.5 gigaoctets in 2017; 2.3 in 2018).

Another piece of information must also be taken into account: the overwhelming dominance of the leader Orange in this corporate market. In 2020, the ARCEP chairman declared that "Orange is too powerful in the corporate mobile market"[10], with a market share of about 60%, and 20% for SFR. Free and Bouygues share the remainder. This essential data will form the basis of the following analyses, and it will be estimated that Bouygues and SFR[11] (whose market shares are currently growing) together hold about one third of this key market.

10-Sébastien Soriano. Interview in Les Echos, 6 Feb. 2020. Since then, these figures have been contested by Orange.
11- Users of Huawei 5G base station and antennae.

B.5 TIMELINE FOR BUILDING 5G NETWORK

In the wake of the 5G licenses that were assigned by auction in September 2020, ARCEP began to grant regulatory permissions authorising operators to activate antennae in a given geographical area on a case-by-case basis. The first implementation occurred in the town of Nice (in November 2020 by SFR) and is expected to be completed step by step in other towns. Four operators obtained 5G licenses (Orange, Free, SFR and Bouygues) for a duration of 15 years, at the following prices :

ORANGE	SFR	FREE	BOUYGUES
EUR 854 million	EUR 728 million	EUR 602 million	EUR 602 million

The fees for obtaining the four licenses granted by ARCEP will be subject to payments spread over time (over a period of 15 years for the 50 MHz blocks, and 4 years for the 10 MHz blocks). Each of the four operators are due to follow a set-up program :

3.000 5G antennae	8.000 antennae	10.500 antennae
before the end of 2022	before the end of 2024	before the end of 2025

During an initial period, the implementation of the infrastructure will be a 5G “non-standalone”, focusing on the installation of the 5G antennae but not on the 5G core network (they will continue to use the 4G core network for a period).

The timetable established by the public authorities foresees several milestones :

- 2020: At least one town for each operator
- 2026: Two thirds of the population living in urban or strong economic areas receiving 5G[12]
- 2030: Fully completed 5G network

12- Source: ARCEP. In 2019, the planned date was 2025. The 2020 target date has also been postponed; at first, two towns for each operator were planned.

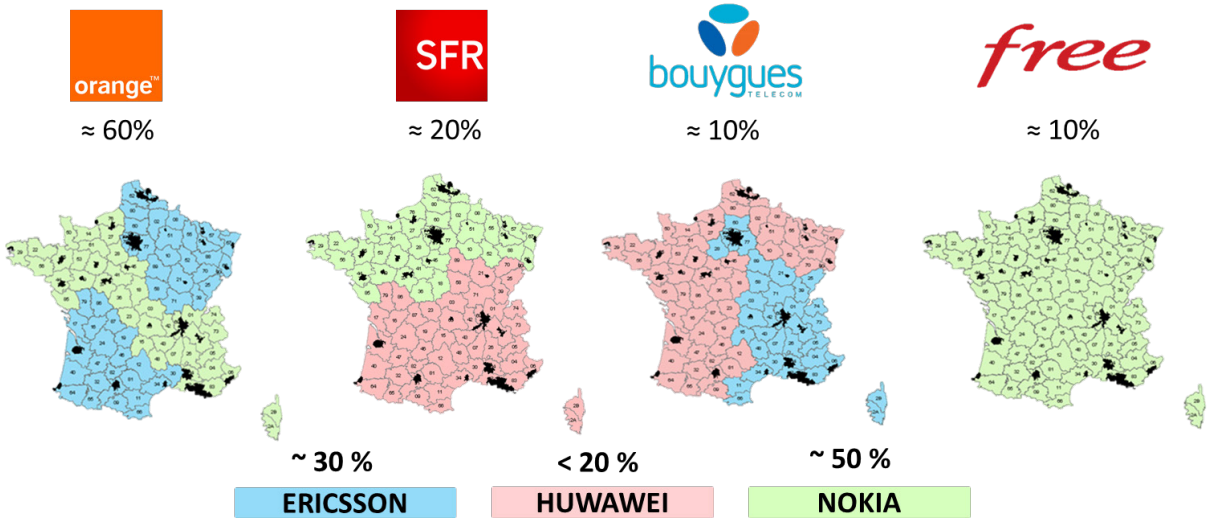
B.6 EXISTING LINK OF TELCOS WITH NETWORK SUPPLIERS

As detailed in the table below, the French telecom market relies on only three suppliers : Nokia, Ericsson and Huawei. In the market of 4G telecommunications, Huawei had, in 2018, a market share of about 20%.

Only two operators – SFR and Bouygues – are currently using Huawei equipment.

- Free recently decided not to buy 5G equipment from Huawei. Before this, Free considered sourcing from one or two new suppliers, and tested Huawei's 5G equipment. By way of comparison, Monaco Telecom, the main telecom operator of the principality of Monaco, which is majority owned by the same company, uses mainly Huawei 5G equipment.
- Orange has experimented with several Huawei 5G antennae, but specified that this didn't include core network equipment.

	Ericsson	Huawei	Nokia
Orange	55.6%	0	44.4%
Bouygues Telecom	52.5%	47.5%	0
Free	0	0.7% [13]	99.3%
SFR	0	52%	48%



Mobile Telecom Landscape and market shares (B2B)[14]

In December 2019, the French government adopted a series of measures (Article L. 34-11 of the French Post and Electronic Communications Code) to regulate the activity of 5G equipment suppliers to preserve national security in the context of mobile radio networks operation.[15] The regulation applies to software and hardware components that ensure, within 5G mobile radio networks, the authentication of terminal equipment, the allocation of radio resources to such terminal equipment, and the routing of their electronic communications between them or to third-party net-

13-Since then, Free has not obtained authorisation from ANSSI to deploy Huawei 5G equipment (2020).
14- Adapted from the French senatorial report n° 579 (2018-2019) by Mrs Catherine PROCACCIA: https://www.senat.fr/rap/l18-579/l18-579.html.
15- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039455649/

works.[16] The reference names in the international standards associated with 5G mobile radio networks, as published by the 3rd Generation Partnership Project (3GPP) of the concerned devices, are listed below :

- New Radio Base Station (en-gNodeB et gNodeB)
- Access and Mobility management Function (AMF)
- Authentication Server Function (AUSF)
- User Plane Function (UPF)
- Session Management Function (SMF)
- Policy Control Function (PCF)
- Network Slice Selection Function (NSSF)

In November 2020, the ANSSI director told a Senate committee that this list is likely to evolve to adopt to technological progress and new risks.[17]

The adopted regulation aims to make 5G-sensitive and critical equipment in the core network or on its main arteries subject to authorisation to prevent them being used for instance as a Trojan horse by foreign malicious entities. Since the publication of the regulation text, ANSSI, which is in charge of delivering these authorisations, received 157 applications from the four telecom operators (Orange, Bouygues, Free and SFR). The applications covered almost 65,000 pieces of equipment and concerned only base stations (i.e. antennae), not core network infrastructure that remains in 4G.[18]

The plan is that ANSSI will provide an answer within two months, with a silence meaning rejection. The table below summarises the status of the submitted applications. [19]

Among 157 applications for 5G equipment authorisation		
82	**53**	**22**
Were granted for the maximum term of 8 years	**Were granted for less than the maximum duration**	**Have been rejected**

In practice, all rejected applications and all “reduced duration authorisations” concerned Huawei equipment.

16- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039455672/
17- Hearing before a Senate committee – Nov. 2020 (Commission des Affaires Etrangères, de la Défense et des Forces Armées)
18- Based on a report from the « Commission des affaires étrangères, de la défense et des forces armées »
19- https://www.senat.fr/presse/cp20201119b.html

B.7 EXISTENCE OF A PRECEDENT FOR CHANGE OF SUPPLY

In 2013, the French state successfully requested that three telecom operators in French overseas territories dismantle their Chinese equipment.

- Orange, which had relied on Huawei on Reunion Island and Mayotte since 2009
- Outremer Telecom (16% of the market shares in French overseas territories), which acquired equipment from ZTE in 2006 for the French West Indies
- Pacific Mobile Telecom had Huawei equipment in Polynesia (these Huawei antennae were replaced by Alcatel ones in 2013)

These three companies used Chinese equipment for their core mobile network. ANSSI had never granted approval to either Huawei or ZTE.

The press highlighted that some of these operators would have obtained important supplier credit to ease their investments, such as a EUR 20 million credit from ZTE to Outremer Telecom.

C-COMPENSATION MEASURES

As a quantitative landmark in the controversy, the chairman of Bouygues telecommunications declared in February 2020 that a "high-performance mobile network in France costs from 8 to 10 billion euro".

Two operators, SFR and Bouygues, initiated legal proceedings in 2020 against restrictive measures imposed on the Chinese equipment manufacturer in the 5G market. The proceedings developed two main arguments:

- Material damage. In February 2020, Martin Bouygues, chairman of the Bouygues Group, declared that " dismantling and reinstalling installations has consequences in terms of costs and delays." (The group says it will be obliged **to dismantle 3,000 5G antennae and base stations in urban areas before 2028**, resulting in a need to also remove the Huawei 4G and 3G that already exists on these sites). This comes with an additional **risk of loss of customers and loss of reputation.**

- Distortion of competition ("fairness of competition" – Bouygues chairman, Feb. 2020) between operators who had Huawei equipment and are now obliged to dismantle them, and those who did not have Huawei equipment. Bouygues is also invoking the legal principle of "equality before public charges", which can be envisaged as a first step to appropriate activation of administrative compensation. The debate also concerns freedom of enterprise.

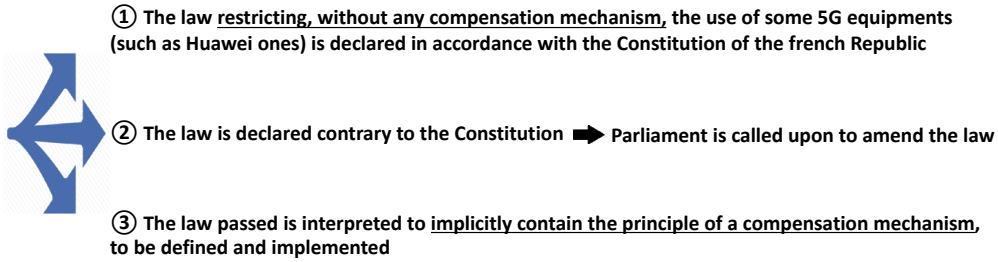
Bouygues referred the matter three times to the Council of State (Conseil d'Etat, the highest administrative court in France). The first two were rejected during the summer of 2020. The third was held in September and questioned the constitutionality of the texts limiting the use of Huawei equipment, at least implicitly, to obtain compensation from the State[20].

In September 2020, the Minister of Digital Affairs Cedric O declared that "there is no negotiation with operators about financial compensation. (…) There is no provision for compensation for decisions that have been made". Conversely, the French federation of telecommunications and SFR referred to the proposal, which they see as a precedent, by US

20 - https://www.reuters.com/article/us-france-huawei-5g-security-exclusive-idUSKCN24N26R

lawmakers of a USD 1 billion fund to help small and rural American wireless providers to root out suspect network equipment provided by blacklisted entities such as Huawei and ZTE, and to replace it with more secure equipment. This assistance will be in the form of a grant, and the Federal Communications Commission will also provide assistance to rural wireless service providers. The comparison made by French operators is reinforced by the fact that in France, too, the recipients – Bouygues and SFR – would also be small companies in the corporate market compared to leader Orange.

In November 2020, the Conseil d'Etat examiner took the first position in favour of compensation for the benefit of Bouygues and SFR, awaiting a final decision. It has also transmitted to the Constitutional council (Conseil constitutionnel, the highest constitutional court in France) the question of the lawfulness of the impugned text. The Conseil constitutionnel was due to take a position on this text at the beginning of 2021, with three possible options :



If options 2 or 3 had been retained by the Conseil constitutionnel, a compensation process would have been instituted, paving the way for the negotiation of amounts.

Declarations and echoes collected seemed, before any negotiation, to mention amounts likely to converge:

- SFR and Bouygues both evaluate this prejudice within **a range of several hundreds of million euro and one billion per operator** (including commercial impacts such as loss of customers)[21].
- State services seem to estimate, at first glance, **hundreds of millions of euros**, but still dispute the notion of compensation.
- These figures appear to be relatively aligned with the **GDP 500 million** (over the next five years) estimation carried out by BT in Great Britain, following British limits on Huawei.

In February 2021, the Conseil constitutionnel decided to validate the parts of the law which had been the subject of complaints, and so to reject these complaints. The Conseil declared that this law "has not transferred to private people (or private companies) expenses which, by their nature, should be borne by the State."[22] This seems to put the costs of dismantling at the charge of Bouygues (3,000 antennae. Other sources of information mention 5,000 antennae) and SFR (up to 8,000, depending on the sources). Such a decision on the question of legality of the French text, however, does not necessarily close the debate and may not stop further legal action.

The figures that circulate in the debate about the cost for replacement of a base station and its antennae are in **the range of EUR 15,000 euros (basic equipment) and EUR 100,000** (taking into account in the latter the need for an operator that would replace the Huawei 5G equipment to make the whole site compatible with the new equipment, which means having to change also the previous Huawei 4G and 3G devices).

The debate will probably remain ongoing, even if it seems to be moving away from a possible settlement of a financial nature between the state and the applicants.

It is important to point out the role in France of several independent administrative or legal bodies on such contentious cases and in compensation settlement processes, such as the Council of State or the Court of Auditors

21- 5G: Bouygues Telecom et SFR demandent une indemnisation de l'Etat si Huawei est exclu". Magazine Phonandroid, 10/03/2020.
22- Décision n° 2020-882 QPC, 5th of February 2021. https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2020882qpc/2020882qpc.pdf https://www.conseil-constitutionnel.fr/node/22757/pdf

(Cour des Comptes, the observatory for effective public expenditure management), since their opinions have already given rise to agreements in previous similar disputes :

◆ Example of the role of the Court of Auditors on a similar file: the early shutdown in 2020, for political reasons and upon decision of the government, of the 1800 megawatts Fessenheim nuclear power plant in Alsace, about ten years before the scheduled end of its actual life cycle, has given rise to controversy about the compensation to be granted to its owner and operator, EDF Group. In 2016, the government proposed eighty to one hundred million euro maximum. This amount was more than twenty times less than what EDF had expected, i.e. EUR 2 billion to compensate for loss of earnings. After negotiation and a parallel threat of legal action by an association for the defense of EDF shareholders against the state, an amount of EUR 377 million euro has been agreed upon. In 2019, the protocol signed between the state and EDF has triggered "a one-off payment of the compensation due for the closure" (instead of an alternative payment solution that would have spread the payments over four years or at the end of this period in 2024, but would have cost more. The choice of immediate payment followed the recommendations by the Court of Auditors, having calculated that a one-off payment after four years would have cost EUR 73 million more).

◆ Example of the role of the Council of State in the Fessenheim file: in 2018, the Court rescinded a 2017 decree deciding upon the closure of this nuclear plant, on the grounds that it was not legally taken. The public authority was forced to start the procedure again. The application for annulment had been filed by local authorities with the argument that the plant's closure would result in a direct loss of EUR 48 million for the local tax system, including 14 million for local authorities (This figure does not include indirect economic damage or damage to other actors). To this end, the **state created a compensation fund** which will be active over ten years.

In summary, with regard to law, jurisprudence and contractual practices in France, it can be noted :

◆ Cases with a similarity to the current 5G case end up giving rise, in many cases, to a sum agreed at the end of a legal match. An example of this legal-economic arm-wrestling arose from the renunciation by the public authorities in 2016 of their truck taxation project ("eco-tax"), which had previously necessitated the installation of electronic check gates on motorways by a Franco-Italian private company called Ecomouv'. The principle of EUR 800 million compensation was contractually agreed upon at the outset of this infrastructure project. But Ecomouv''s threat to sue the Council of state was said to ask for compensation within a range of EUR 1 and 1.5 billion, for "renunciation of contract", loss of income and damage to image. At the end, the indemnification took the form of an immediate payment of EUR 400 million followed by a EUR 40 million annual installment over 10 years to compensate for the debts of Ecomouv' to banks incurred by this project.

◆ The option of compensation by the state may give rise either to direct or indirect – by means of a dedicated fund – payment, to immediate, staggered or on fixed date payment.

C.2 COMPENSATION BY THE INSURER'S ASSUMPTION

With regards to financial compensation, the French insurance industry, and more specifically the French Federation of insurers (FFA, a professional organisation and joint body that brings together most of the insurers and reinsurers active in France), has not yet positioned itself openly on this subject. The usual point of view of this profession on such situations is that it is the responsibility of the state, whose application to dismantle Huawei's telecommunication facilities put this public authority in the frontline for paying any compensations or damages concerning removal expanditures and related costs.

The operators and the French Federation of Telecommunications (FFT, a professional union that brings together the operators active in France) adopt the same point of view.

With regards to the risks faced by their own clients (potential threats such as telecommunication interception or blockage, cyberattack facilitation, determination of the location of a person or a vehicle, etc.): if it transpired that several telecommunications operators overrode the state recommendations or prohibition, an insurance company would consider that such risk-tacking would exempt it from its contractual obligations and of any insurance coverage. Consequently, and unless there exist specific clauses previously agreed between a telecommunications operator and its insurer, the latter will usualy consider that :

- There is no presence of material damage sustained by the operator (no destruction such as glass breaking or fire, no theft, no physical forced intrusion at the home of a person, etc.) but only of additional costs juridically somewhat comparable to an expropriation or a land reparcelling decided by the public authority;

- There is the presence of potential civil liability but that will, in principle, not be covered by insurance, as a result of the disobedience that generates the injury, if it happens, suffered in the future by the operators' clients. If these clients decide to start a lawsuit or to initiate contractual penalties, the operator's insurer will consider itself released from any obligation to cover the expenditures.

More generally and with regard to any kind of cyberattack, the insurance industry has become more careful in recent years and it is unlikely that it would, without controversy, cover damages by the customers of these operators if these attacks have been facilitated by intentional vulnerabilities in 5G equipment from untrusted vendors, the probable existence of which was long public.

D-ESTIMATION OF SECURITY-SENSITIVE SECTOR

With the aim of containing such costs and potential hazards, French authorities in 2020 adopted or reinforced several key measures to protect and preserve security-sensitive actors from exposure to untrusted vendors and equipment.

◆ One measure is **quantitative** and seeks to limit the number of operators authorised to be supplied by Huawei by refusing to allow operators to build supplier relationships with Huawei unless they already existed previously, for example with 4G (Guillaume Poupard, director of ANSSI, declared that "the operators that don't use Huawei, we do not encourage them to start"). This decision affected Free, which had initially put Nokia, Ericsson and Huawei in competition during its call for tender concerning 5G. Free announced in September 2020 that it has been refused by ANSSI to contract with Huawei. This decision results in an unusual situation due to the fact that the prices offered by Nokia and Ericsson are probably below what they would have been if they had only been two, instead of three, in competition.

◆ A second measure amplifies a global **geographical** approach, which was previously taking shape by an unwritten rule, prescribing against installation of any security-sensitive telecommunication equipment or device provided by a supplier over which there remain uncertainties (any incomplete trust), when too close to places of political power, especially in Paris near state, parliament or government departments (this unofficial request particularly applied to core network equipment). The recent formalisation and strengthening of this unofficial rule is divided into two ratings:

The strategic character of an area will be defined, for example, by the presence of:

• Sensitive military areas: Bouygues now plans to dismantle its already installed Huawei antennae in the neighbourhood of the French naval base in Britanny (town of Brest and its nuclear submarines site) and of a military research centre dedicated to cyberwar (Town of Rennes).

• Industrial areas: the same antennae will be dismantled in the neighbourhood of Airbus plant – HQ and factories – in the town and suburbs of Toulouse.

• Political centers, such as Strasbourg, where the European Parliament is located. Perhaps incidentally, the Strasbourg conurbation also hosts several cybersecurity competence centers.

The first tranche of this program will concern :

Bouygues	Said to be = 3000 antennae	Before 2008 and out of a total of 21,500
SFR: The figures are not published	Said to be > 3000 antennae	Before 2008 and out of an approximate total of 23,000

The timeline for the uninstallation already begun in 2020, with the dismantling of Bouygues' antennae located in Strasbourg. In the months to come, Brest, Toulouse and Rennes will continue the process, followed by several other towns over the coming years (at least 11 more, apparently Pau, Nice, Nancy, etc.).

◆ A third approach is **demographic**, and results in Huawei equipment being avoided in densely populated areas, such as Paris. A consequence of this approach is less stringency in sparsely populated regions or areas without technological, military, security or political issues.

The Huawei market share in French 5G, which is a moderate number in itself, will be, in addition, circumscribed to lower-risk areas (geographical aspect) and to lower utilisation rate areas (demographic aspect).

◆ A fourth dimension depends on the **criticality** of the service – energy, transport, telecommunications – provided by some economic or institutional players (see explanation about OIV and OSE below). The criticality of their product or service requires them to avoid unnecessary risks by procuring from untrusted sources.

E-POTENTIAL COSTS OF ANY MALICIOUS VENDORS

E.1 OBVIOUS COSTS : ESTIMATE OF POSSIBLE SABOTAGE / INTENTIONAL OUTRAGE (see appendix n°1)

E.2 HIDDEN COSTS : ESTIMATE OF POSSIBLE DATA BREACH BY 2030

Two main operating methods can be envisaged with regards to espionage throughout telecommunication equipments :

- The passive method, which simply consists of intercepting communications transmitted by this equipment.

- The active method, which means that any company monitoring and maintaining telecommunication network equipments would have the facility to implant malware, such as sniffers or other espionage software, into customers' devices, and to then remove data from the victims' computer system.

The true number of espionage cases and data breaches in France, by means of telecommunication equipments, is not easy to evaluate: the quantity of data breach notifications, made mandatory by the 2018 Personal Data Protection Act, counts 2159 notifications in 2019 which, according to the modeling adopted, would result in annual damage close to EUR 560 million in 2022. However, this low number of notifications – in comparison with other countries, such as Germany or the Netherlands – gives rise to the question of its degree of representativeness of reality on the ground. It is possible that this number is underrepresentative. On the basis of the probably more reliable figures from Germany, and weighting them by the difference between German and French GNPs, such an alternative approach would result in an estimate of 17,525 notifications, and an annual prejudice of 4.5 billions of euros.

Even if they were exhaustive, notifications could only represent the visible part of the attacks. The portion detected by victims or by law enforcement authorities are only the tip of the iceberg.

PROSPECTIVE ANALYSIS FOR THE 2030 TIMEFRAME

The cost of companies' data breaches is also for the most part unknown in France, especially because important information regarding complaints about cybercrime or espionage are not publicly available. However, two complementary landmarks will help to build an estimate range :

- **" Maximum " unit cost:** an IBM-Ponemon study [23] suggests an average cost for France of data breaches to a magnitude order of EUR 4.4 million per breach in 2019, but its sample mainly represents big or middle-sized companies (only 13% under 500 employees).

- **Minimum unit cost:** another recent study [24] highlighted that, for the vast majority of small and very small companies (except start-ups, small high-tech companies or subcontractors of strategic companies, which represent a total of some tens of thousands of companies), the impact of a data unavailability – for example, because of a ransomware – is high; but on the contrary, the impact of data being simply copied or intercepted without destruction is often low because of low value to others of, for exemple, the monthly accounting data of a small automotive repair company. Some of them have an actual use value, such as a customers list or a price list to build quotes, but if they are simply copied, the magnitude order of the prejudice for this majority of French enterprises – the small ones – would be an approximate average cost equal to or less than some thousands of euros; that is to say, the thousandth of big companies unit costs (once again, EUR 4.4 million).

23- IBM-Ponemon "Cost of a Data Breach" 2020 Report.
24- IRT-SystemX research Program and report: « Les cyberattaques: quels préjudices sur les entreprises et sur l'economie ? ». 2019.

It should be noted that, since the average turnover of most small companies is below one thousandth of the average turnover of the big ones, it makes sense that the damage suffered by small companies (in this case, a data theft) will also be about one thousandth of the damage suffered by the big ones.

◆ **Average cost calculation for all companies:** considering that the Ponemon sample indicates an average prejudice of EUR 4.4 million for the category of big and middle-size companies, which includes about 5000 enterprises in France (1.25‰ of the total number of French companies), but which generates about 45% of the national value added (GDP):

- If all 5000 companies were hit, the cost would represent 5000 x 4.4 millions = EUR 22 billion.

- If all French companies, representing 100% of the national value added, were hit, the cost may represent EUR 22 billion x 100%/45% = EUR 48.9 billion, rounded to EUR 50 billion that could be named "Maximum possible loss".

Nevertheless, supposing that all companies (100%) would be hit is a hypothesis too highly implausible, which leads us to build two more probable scenarios:

First hypothesis: assumption of random interceptions throughout 5G

Each "1%" of victims beyond the companies would mean EUR 0.489 billion of prejudice. The question then raised will be to evaluate the percentage of interceptions for each country (see below).

Second hypothesis, more likely in the long run: assumption of targeted interceptions throughout 5G

The attacks would be here rationally targeted towards the most valuable prey. It has been observed that if the attacks only focus on the 5000 main companies, it may cause a prejudice of EUR 22 billion; but this tiny percentage (1.25‰ of the total number of companies) include, in fact, about 40% of the workforce in France – in the private sector – which would therefore imply a very large-scale surveillance operation of millions of employees.

- However, spying on their internal telecommunications would require intercepting less than 40% of the business telecommunications. We can consider roughly that intercepting about 30% of the telecommunications would be sufficient.

- Only the most interesting employees -researchers, managing staff, experts, and so on- would be priority targeted, and are few in number. What's more, the redundancies (Let us recall that there are at least two persons participating in a phone call) are very important within these sub-categories; researchers use the phone to call researchers, as well as business lawyers or chartered accountants. Moreover, email attachments are the best targets for data theft, and are easily identifiable in telecommunications flows.

One conclusion is that efficient targeting of, for example, 1% of employees (the most interesting ones) within 1% of the companies (the most interesting[25]) results in a minimum statement of billions of euro of prejudice per year, at the expense of France.

If we suppose that researchers, managing staff or experts represent, very approximately, 5% of the workforce of these most interesting companies, it would only take 30% x 5% = 1.5% of the whole French workforce to be wiretapped: with an efficient targeting (a "perfect targeting") of 1.5% of business telecommunications, targeted intercep-

25- There may sometime be a need to swap a big non-interesting company with a smaller but more attractive one, while remaining at the same total of 5000.

tion would cause France damage of about EUR 20 billion.
This would be the case if a supplier's antennae, base stations and core networks were the only deployed in the country. However, for example Huawei will only provide 15 to 20% of the 5G antennae implemented in France – and no core network – confined to non-urban and non-industrial areas. These quantitative and spatial precautions are a risk reducer, which can be estimated to be around a factor of ten.

- By 2030, when the 5G generation has been deployed, a reasonable assessment of maximal risk retains a range of **EUR 1 billion < ? < EUR 3 billion per year**, when focused on the 5000 most interesting French companies.

Several other elements must be taken into account to refine this costing[26]:

- The Ponemon study numbers help provide a benchmark, but does not pretend to perfectly represent the specific impact of a telecom interception, nor express a maximum of prejudice causable, or a maximum number of prejudice per victims.

- The telecommunications of businesses are in the minority of the total communications flow, although this information should be put into perspective, because many employees use their personal mobile phone for professional conversations.

26- Additionally, a phone call between two mobile phones usually activates two different antennae.

F- OTHER HIDDEN COSTS

F.1 PREVENTION AND CONTROL

The growth of ANSSI's current workforce (600 people) is made necessary by the development of its missions (security of the state's information systems, operators of vital importance and of essential services, implementation of the law on the security of 5G networks, etc.).

From the perspective of a research center created ex nihilo, the staff required to satisfactorily test and control the security of the telecommunication devices implemented in France can be estimated at **150 multidisciplinary experts** (minimum to be efficient): high-level engineers and lawyers would work together in order to check also the commercial contracts, verify if technical documentation and translations provided by suppliers of foreign origin are sincere and faithful to reality, and prepare legal texts. The total desirable payroll therefore tends towards an approximate and minimal range of EUR 12 and 16 million per year, to which operating costs must be added. With the expansive technical means due to be allocated for such a mission (laboratory, test beds, etc.), **the total desirable budget in the case of untrusted telecommunication suppliers may be considered around EUR 30 million per year** (In a rather similar role and as a benchmark, the budget of the IRT-SystemX research center is EUR 23 million per year).

It should be emphasised that telecommunications engineers or lawyers are precious and rare resources. It is estimated by French universities and colleges that the number of future engineers to be trained to meet needs already has to grow by a ratio of 50%.[27] Consequently, the need to compensate for a lack of trust in digital devices by hiring new staff generates two economical nuisances :

- It mobilises a significant budget paid by the French taxpayer (and consumers of telecommunication services);
- It increases the salary inflation and the scarcity of human skills on the telecommunication and sofware job market, to the detriment of the French companies.

F.2 REGULATORY COSTS

These costs, which interfere with the prevention and control costs above, could be estimated at about EUR 3 million per year in the first instance, but are progressively proportionate to the needs revealed by the technical test center for legal and regulatory complements. This amount does not apply only to the enactment of law, but also to the monitoring of contractual relations between operators and unstrusted suppliers.

It doesn't include the additional efforts made by French private companies to protect their data -such as encryption –, their telecommunication use, and to verify compliance with data laws.

In the French legislative procedure, drafts of national laws are accompanied by an impact study when they are transmitted to the parliament. The purpose of this impact study is to assess the economic, financial, social and environmental impacts of the future law before its consideration by the two houses of parliament. This evalution is overseen by the minister responsible for introducing the law project. However, the financial dimension of such studies only evaluates the direct impact on the state budget and corresponding ministers, and does not assess the cascading impacts that may affect societies, organisations and individuals. For instance, Article 22 of the French Military Programming Law (LPM) adopted on 19 December 2013 obliges operators of vital importance (OIV) to comply with several cybersecurity requirements such as : compliance with specific security rules, use of qualified equipment and service providers for the

27- Conférence des directeurs des écoles françaises d'ingénieurs (CDEFI)

detection of security events, mandatory notification of security incidents, regular security verifications, and technical audits performed by the ANSSI. In this case, the regulatory impact assessment evaluates only the cost of the human and technical resources required to enforce and control the new regulation and apply penal sanctions to non-complying OIVs **(EUR 150,000 for the OIV director and EUR 750,000 for the legal entity).**

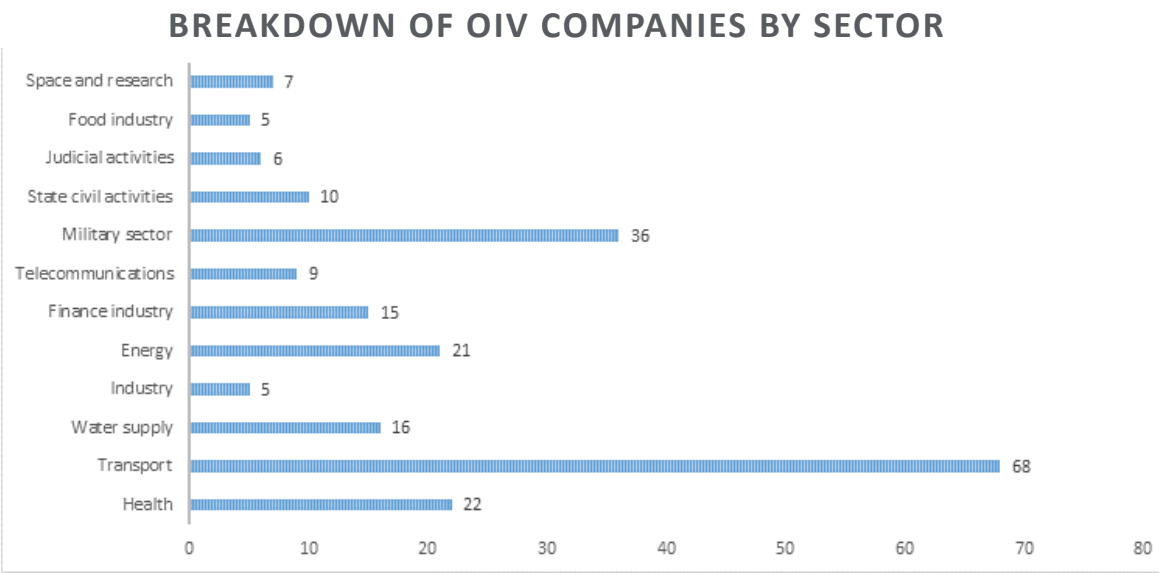
Nevertheless, operational extra costs needed by each OIV to comply with the regulation are hard to evaluate. While the sensitive information system (SIS) is estimated to represent 3% of the complete information system of an OIV, **the budget needed to conduct the compliance with LPM ranges from EUR 5 to 45 million.**[28]

F.3 SHIFT OF DEMAND

Two different risks exist:

- The figures concerning a first risk – of customer loss or of decrease in satisfaction of clients because of any future necessity to stop using, for example, Huawei 5G equipment - isn't published by operators, but seems to be estimated by them at hundreds of millions of euro if the permutation of materials is permitted to take place gradually and calmly. If the necessity to stop using this equipment was urgent and accompanied by important media coverage detrimental to brand image, the prejudice would become more substantial.

One of the worst scenarios envisages that economic or institutional players providing services that require a high level of security (criticality of the service) stop using untrusted suppliers or sub-contractors. From 2013 to 2016, France was maintaining a list of 200 to 300 entities considered to be "Operator of Vital Importance" (OIV). (An "operator" can be any company. The word is unrelated to telecommunications operator).



In 2018, the country adopted and published the national transposition of the NIS directive.[29] A first list of 122 "Operators of essential services" (OSE) has been drawn up, and is in the process of being completed by two other lists. While the list of OIV and OSE remains secret, their number is estimated to have reached 600 companies in 2020.[30] OSE and OIV are subject to the same type of requirements as the LPM, used as a basis for the NIS directive. If they are obliged to leave untrusted suppliers, the approximate loss of revenue would be high for them.

28-Synetis study. https://www.synetis.com/lpm-reussir-la-mise-en-conformite-de-ses-systemes-dinformations-dimportance-vitale-siiv/
27- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036939971/#JORFSCTA000036939986
29-https://www.solutions-numeriques.com/securite/cybersecurite-bientot-600-operateurs-dimportance-vitale-oiv-et-de-services-essentiels-ose/

The OIV list is unpublished, but we can estimate their percentage at roughly 20% of the French GDP (therefore they may be also in the clientele of SFR or Bouygues, who will incur the risk of seeing this customer base shifting towards trusted equipments and operators).

	Annual turnover (fixed and mobile communications)	**Estimated annual turnover on corporate market** (mobile communications)	**Estimated turnover with OIV** (mobile communications)
Bouygues Tel.	EUR 6.06 billion (2019)	EUR 230 million	EUR 50 million
SFR	EUR 10.1 billion (2018)	EUR 460 million	EUR 100 million

The evaluation above takes into account the percentage of MNO corporate customers (18%) and the subpart of the OIV (20%) within this category. Alltogether, **a maximal shift of demand would represent an amount of about EUR 150 million per year. Adding the OSE would** increase this first amount and make it **tend towards EUR 250-300 million.**

Criticality also relates to the intellectual patrimony and property of companies ("IPR-intensive industries"), even non-strategic ones, from a geopolitical point of view, and more specifically to their know-how, their research in progress. All confidential data related to innovations or commercial negotiations is pillagable. Evaluating the potential shift of demand triggered by IPR-intensive industries is difficult, because an important percentage of them are also members of the above OIV and OSE (the lists of which, it should be remembered, are kept secret in France). But this not easily measurable shift would contribute to inflating the previous amount - of about EUR 250 or 300 million - and make it exceed by a wide margin the threshold of EUR 300 million per year (out of a probable total of about EUR 1.200 million for the global OIV and OSE and IPR segment, for all French operators. The evaluations carried out using our calculation guidelines, and depending on the magnitude of the overlap between OIV, OSE and IPR intensive industries, result in an outcome of EUR 474,880,000 -OIV, OSE- and EUR 1 billion -IPR-, which can be seen as a ceiling estimate).

The reason for this departure of an IPR-intensive clientele is that it will find itself in fear of being dispossessed of these competitive advantages because of potential telephone tapping. Rather than an impossible cash settlement of the damage of industrial and commercial espionage, it would be more appropriate to count with other measurement tools. Considering that **42.5%**[31] **of French GDP is generated by economic sectors that have the most recourse to intellectual protection** (patents, drawings, trademark registrations), and that these sectors are the most dynamic in job creation and in the field of new business creation, any attack against this intellectual capital :

- is a destroyer of growth vectors. Growth is probably the best marking tool: a telecommunications infrastructure capable of capturing some tens of per cent of all the communications – or at least to search in – is in a position to target an important part of the information carrying either future innovations or upcoming commercial contracts.

- is a destroyer of job creation. Fine figures remain handicapped by our ignorance of the recycling part of industrial espionage via ICT; as an imperfect benchmark, research conducted predict 30,000 to 40,000 jobs being destroyed in France annually by counterfeiting, and a loss of EUR 6 to 10 billion for the national economy[32], but such practices have other non-digital means at their disposal. On the other hand, direct counterfeiting is only a small visible part of the consequences of technological espionage.

31-https://www.linfodurable.fr/les-secteurs-utilisant-fortement-la-propriete-intellectuelle-pesent-la-moitie-du-pib-de-lue-etude
32-https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-economique-et-commerce-exterieur/peser-sur-le-cadre-de-regulation-europeen-et-international-dans-le-sens-de-nos/faire-de-la-regulation-internationale-un-atout-pour-l-economie-francaise/article/lutte-contre-la-contrefacon-et-le-piratage

Regarding the latter marker, it is of interest to highlight that it is, at least, of the same order of magnitude as our current low growth and low job creation. The great discretion of telecommunication interceptions allows their duration and their profusion, so it can be conceived as a slow impoverisher, destroying the future more than the present.

- The figures concerning the lawsuits brought by the customers of an operator if the threat above materializes, would be of a lethal nature for this operator.

F.4 NEED FOR REDUNDANT TELECOMMUNICATION INFRASTRUCTURE

About private sector telecommunication networks : state authorities and the main sensitive companies have maintained a privileged and special link to the historical operator (Orange, the biggest operator in France, and especially in the corporate market) that was in the past state-owned, and has no Huawei base station or antennae, nor 4G nor 5G. What's more, as a rescue solution, another operator – Free – has no such Huawei equipment, and has been refused by ANSSI to buy it. Together, they have about 70% of the corporate mobile market.

About public sector telecommunication networks : several French state-sensitive institutions used for a long time, and in parallel ways, their own mobile telecommunication networks (2G Acropol for police, Rubis for gendarmerie, Antares for fire departments and security services, etc.). Altogether, these state-owned networks probably have about 300,000 users. Their existence forms part of an already long history:

- In the beginning of the 1990s, police and gendarmerie adopted digital technologies instead of former analog telecommunications.
- In 2006, a pooling system (INPT, a shareable national communications infrastructure, whose deployment is designed to last 10 years) started to be implemented between these various independent networks, covering about 95% of the French territory. Since then, several parliamentary reports have nevertheless brought to light a drift of budgets.[33] The budgets devoted for improving INPT since 2017 amount to EUR 140 million.
- In 2014, another step was the development, with the help of ANSSI, of mobile phones able to use both these state telecommunication networks or the private ones provided by the MNOs. These mobile terminals use VPN, digital certificates and communication encryption. Orange Business Services, which doesn't use Huawei equipment, has been awarded the deployment contract. None of the 80,000 personnal phones already purchased is Huawei.

A further step will cause a paradigm shift because it will be backed by private operators. It is called RRF – radio network of the future. This 7-year project (design and experimentation) will include, among its users, some staff of the OIV, which are 250 security-sensitive companies (energy, transport, etc.) generating about 20% of the French GDP. The global budget is estimated at EUR 166 million.[34] Therefore the designing and testing of this new upcoming technological generation, in preparation since 2017 and planned until 2024, corresponds to an average budget of about EUR 20 million per year.

The networks that already exist require constant upgrade and reinvestments in new generation technologies. Despite a high margin of uncertainty, a rough estimate will retain an OPEX ≥ EUR 250 million per year, and a CAPEX ≥ 200 million per year.

RRF has been planned to make it operational for the Paris 2024 Olympic games. However, if it is true that the existence of untrusted telecommunication providers reinforces the interest of redundant infrastructures, their weight is not assessable in the decision to implement RRF.

Altogether, the total annual cost of EUR 470 million is to be considered as a minimum estimate.

33- « Rapport d'information n° 365 (2015-2016) de M. Jean Pierre VOGEL, fait au nom de la commission des finances, déposé le 3 février 2016: Réseau radio numérique des services de secours (ANTARES) -z

34-https://www.performance-publique.budget.gouv.fr/sites/performance_publique/files/farandole/ressources/2020/pap/html/DBGPGMJPEPGM216.htm

G-TOP-DOWN APPROACH

G.1 OXFORD ECONOMICS REPORT WITH REGARD TO THE FRENCH SITUATION

In addition to its theories, partially questionable, that less competition would result in lesser service quality and less innovation, Oxford Economics refers to some supposed technical necessities that don't appear to be applicable to the French situation :

- The alleged difficulty in replacing one provider such as Huawei only applies to the two smallest operators for a moderate total of antennae (some thousands, during the eight years to come). The whole market share of Huawei in France will only be about 15 to 20%, and furthermore part of this equipment, when in rural areas, is not included in any obligation to dismantle them in the coming years.

- The supposed urgency of implementing the 5G technology in order to be time-to-market is questioned by a growing number of independent experts and actors. This reflection on the real needs and the real rhythm of the market take-off finds support among several operators:
  - The Bouygues chairman put 2023 or thereabouts as the date when, in his view, the actual needs of the market for 5G technology will be expressed. He believed that French operators would not be significantly behind if the speed of launch of the 5G generation was slightly reduced.
  - Gregory Rabuel, general manager of SFR, publicly called (in June 2020) for a rebalancing of priorities in favour of achieving, at first, 4G and optical fiber deployments, and declared "do we need 5G for the short term? This is not sure."
  - Stéphane Richard, Orange chairman, said that he didn't expect any excitement from the customers at the commercial launch planned for the end of 2020, and that he is focused more on the following year.

Most of these operators mention social resistance or hesitations from several local authorities, which will affect the rhythms initially planned. Therefore the effects of a delayed roll-out and the damage to public interest must be moderate, just like the calculations mentioning damages of an amount in billions.

> The Oxford Economics pyramid of numbers is based on an alleged market pace, which remains largely unknown. There is no absolute evidence that France is late instead of early, in which case, the damage would, on the contrary, be caused by keeping up with the recent frenetic and unbridled competition.

The real damage is to be sought among economic and social actors who are victims of bad timing, but prejudging the correct pace in the current economic and technological context would be a wager beyond the scope of a scientific approach.

Regarding an initial feedback that relates to a territory neighbouring France, a recent position on the necessary caution to be adopted with regard to figures and pre-written conclusions seems significant: to the question "were you able to quantify the economic impact (of the 5G on your territory) ?", the Chief Digital Officer of the Principality of Monaco – which had previously inaugurated its 5G network in July 2019 – responded "it is too early to quantify the economic impact of the phenomenon, and the health crisis we are experiencing (COVID-19) distorts any analysis".[35]

35-Fondation Concorde: « 5G: prendre le virage du monde d'après », page 64. Author Nicolas Sironneau ; interview with Frédéric Genta. June 2020.

H-SUMMARY

When it comes to cybersecurity, France has advocated a common approach at the European level. The 5G risk analysis and the toolbox published by the Europen Commission are two excellent examples of common measures that should be applied at the national level. France already complies with this framework and its prudent strategy may be a source of inspiration in regulating the 5G market.

The 5G case appears in France to be part of the long term, and seems to be made up of successive stages that can be described as many balances of power.

- Historically, for national security reasons, the country has always attached great importance to the control and mastery of its telecommunication infrastructures;
- The priority given to safety has slowly diminished since the 1990s, and has given way to competitiveness priorities, mainly focused on prices. This was very visible with the launch of 3G and 4G, and the opening to international competition between suppliers of all nationalities;
- The arrival of 5G caused a relative stop, a break in the previous trend, and a comeback of security concerns. The Huawei strategy for setting up in the French market has undergone containment. Today, the balance sheet in terms of telecommunications protection can be considered as cautious (see below, the "Dependency measurement scale").
- It is likely that the economic stakes will counterbalance previous security concern in unknown proportions. In times of economic crisis, the question will become linked to job creation, to the set up of new 5G equipments production plants in France, or of 5G research centers that would support local employment. The first signs of this future round are already perceptible. Two external factors will probably come into play :
  - The future importance of the feeling of insecurity, if there is confirmation of the risk of interception of 5G communications.
  - The pace of 5G market growth, and of the emergence of new uses. The visibility is low on this future trend, but will have an impact. If the commercial breakthrough of 5G is below expectations, as is believed by many observers and stakeholders, its economic attractiveness in the eyes of the political world may be reduced, in comparison with the security risk.

DEPENDENCY MEASUREMENT SCALE (2021)

Evaluation of the levels of presence of untrusted 5G suppliers in the country

	Measuring scale	French situation review
Number of operators having no untrusted 5G supplier (including the existence of a state redundant network)		
No operator is using exclusively trusted 5G equipment	**3/10**	
A minority of operators are using exclusively trusted 5G equipment	**2/10**	
A majority of operators are using exclusively trusted 5G equipment	**1/10**	**1**
All operators are using exclusively trusted 5G equipment	**0**	
Percentage of consumers having an operator using untrusted 5G equipment in the country		
All consumers	**3/10**	
A majority of consumers	**2/10**	
A minority of consumers	**1/10**	**1**
No consumer	**0**	

Percentage of sensitive areas fitted with untrusted 5G equipments in the country		
All the sensitive areas	3/10	
A majority of the sensitive areas	2/10	
A minority of the sensitive areas	1/10	
No sensitive area	0	0
Presence of core network equipment provided by untrusted suppliers	0 or 1/10	0
TOTAL	x/10	**2/10**

Taking into account this current dependence – if it remains at the same level in the future – and since three scenarios have been considered, it becomes easier to quantify them :

GOLDILOCKS SCENARIO (NO COMMUNICATION INTERCEPTION, NO CYBERATTACK, ETC.)

We expect the French prejudice in this scenario to be moderate, simply adding technical verifications about the safety of devices, and suffering the economic consequences of a propensity to self-censorship among security-sensitive companies (the absence of espionage can never be proved, and doubt always persists).

It represents an annual amount probably in the tens of millions of euro, but its recurrence each year would result in a total amount in the hundreds of millions of euro throughout the duration.

We estimate the global cost over a decade > EUR 300 million minimum.

ARMAGEDDON SCENARIO

The global cost of the worst scenario, if all the means of attack are triggered to their maximum (First, the attack will remain undetected by the victim, and only later will the attack and its damages become visible) would cost at least some hundreds of billions of euro to the French economy (see Annex 1), with the addition of huge human cost.

We consider plausible a destructive impact greater than or equal to EUR 1000 billion, at the expense of France, or, in other words EUR 1 trillion. Such an event would plausibly occur only once.

REALISTIC SCENARIO

In the short term, the minimal cost may be envisaged as hundreds of millions of euro per year.
But in the long term, the cumulative nature of these prejudices would make the final result look like a “slow Armageddon” scenario.

By way of summary, our three scenarios are staggered over three levels of expenditure, and present the paces of an exponential curve :

- The Goldilocks scenario represents a minimum annual amount of tens of millions of euro.
- The Realistic scenario represents a minimum annual amount of hundreds of millions of euro.
- The Armageddon scenario represents a minimum one-shot amount of hundreds of billions of euro.

I-APPENDIX 1

QUANTIFICATION OF POTENTIAL PREJUDICE CAUSED BY ANY FUTURE TELECOMMUNICATION ATTACK:

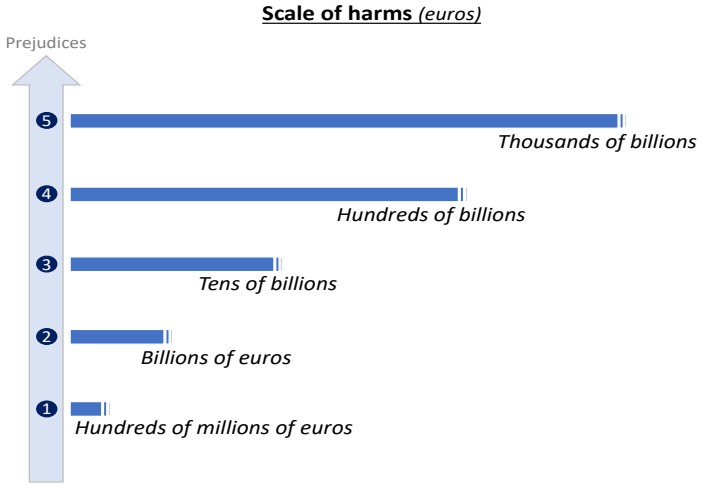
A comparison

of the German, Italian, Portuguese and French exposures

Looking for four orders of magnitude to the 2030 horizon

Considering that many possible variants and scenarios can legitimately claim to describe the dynamics of propagation by a telecommunication attack, and considering also that the rhythm of implementation of the communicating objects – with their degree of interconnection – within the next ten years is hard to anticipate today, our aim is to be satisfied with simple evaluation ranges comparable to a Richter scale. Or, more accurately, to a Rossi-Forel scale; that is to say a scale that doesn't transcribe the strength of the attack, but the size of its consequences.

The Rossi-Forel scale is composed of ten levels. Our one is a **logarithmic scale with five levels**, each one being the tenfold of the previous one.



Our evaluation will rely predominantly on previous estimates[36] obtained from our national study on cryptovirus attacks in France, carried out from 2016 to 2020[37]. DDoS attacks by the means of IoT or other devices that would be infected and brought under control via a 5G equipment are not studied here, due to the insufficiency of statistical references.

The global cost of the cryptovirus attacks in France will serve as a measurement standard.

36- A complementary scenario studied possible cyberattacks in the aeronautical industry supply chain and the difficulties for insurers in taking charge: « Maîtrise du Risque Cyber et Assurance: Scénario cyber s'appliquant à la filière aéronautique. Réponse du marché ». https://hal.archives-ouvertes.fr/hal-02416407

37- IRT-SystemX research Program and report: « Les cyberattaques: quels préjudices sur les entreprises et sur l'economie ? ». About seventy companies victims of hacking (and many other witnesses, insurers, representatives of public authorities, chambers of commerce, etc.) have been met during four years, throughout the whole French territory. In most cases, the meeting were in-house, on the premises of each factory or office attacked, in order to better understand the functioning and the environment of each of these companies. Almost all were SMEs, individual entrepreneurs, or independent associations (profit or non-profit associations). The majority of them had suffered from ransomware. The other interviews referred to phreaking, CEO scam, DDoS attacks, and so on.

ANNUAL COST OF THE CRYPTOVIRUS IN FRANCE

The probability of occurrence of a cyberattack has been ultimately estimated by our study as between 4% and 5% per year (this percentage is one that grows throughout the years). Taking into account the direct costs – below - observed by victims, the following figures have been obtained (we wish to emphasise that they are minimum estimates):

Entrepreneurial sphere

Altogether, the number of French companies is close to 3,700,000 entities – not including agricultural structures. Almost 99% of these companies have less than 50 employees.

4% of victims / year	Enterprises < 10 pers.	Enterprises 10 to 50 pers	Total entrepr. < 50 pers
	3 500 000 enterprises	130 000 enterprises	
Average cost	EUR 6 000 / attack	EUR 15 000 / attack	
Global cost	≈ EUR 840 million	≈ EUR 80 million	≈ EUR **920 million**

Associative world

In addition, there are 1,300,000 active associations.

4% of victims / year	Assoc. w/o employees	Assoc. of 1-50 employees	Total assoc. < 50 pers
	900 000 associations	150 000 associations	
Average cost	EUR 1 000 / attack	EUR 7 000 / attack	
Global cost	≈ EUR 36 million	≈ EUR 42 million	≈ EUR **80 million**

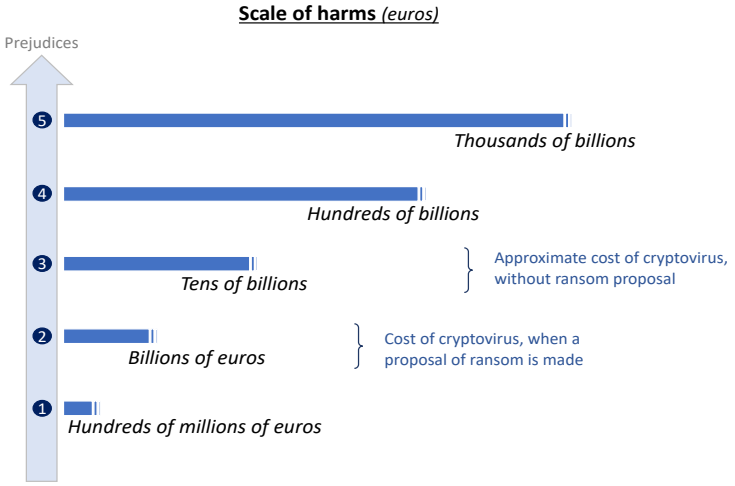
In total annually for companies and associations of fewer than 50 people, the assumption with 4% of victims is close to EUR 1 billion (costs within the victims).

Adding the medium-sized and large firms and associations (> 50 pers.), administrations, public institutions and local authorities, with all the residual imprecision attached to it, results in a minimum estimate of EUR two billion - but probably above - for total enterprises and other socio-economic institutions, to which we must add the indirect costs (to indirect victims, contractors and their subcontractors, clients, partners, etc.). The initial results of our study indicate that the indirect prejudices are of a similar order of magnitude, which constitutes a doubling.

In total, the direct and indirect costs for all companies and associations, the assumption with 4% of victims is close to a minimum of EUR 4 billion in a year (dating from 2018). Again, this is a minimal interpretation.

Referring to our scale of harm below, the global annual cost of cryptovirus cyberattacks can be estimated at a minimum that falls into the category of "billions of euro" (Rank 2).

However, these numbers are affected by a reduction factor that lowers them: an important percentage of the companies suffering from such a ransomware accept paying this ransom as soon as the amount of prejudices starts to grow high. That attitude is diminishing what would have been the real cost without the ransom "emergency exit". Otherwise, if these attacks were without recourse, the final prejudices would tend toward a level situated between Rank 2 and Rank 3 (see illustration "Scale of harms").



Ranks 2 and 3 have been obtained by an attack scenario developed in 2017 by the Lloyd's of London and Cyence[38]. This study "Introduced two scenarios to help insurers quantify cyber-risk aggregation (...): a hack that takes down their cloud-service provider or an attack that causes the failure of a particular operating system across their own company, customers, suppliers and/or business partners ».

◆ The Cyber CSP (cloud-service provider) interruption scenario assessed an impact within a range of USD 4.60 billion (our Rank 2) and USD 53.05 billion (Rank 3).

◆ The cyber mass vulnerability scenario obtained a range of USD 9.68 billion and USD 28.72 billion.

The Lloyd's and Cyence study also referred to the figures published by Hiscox Insurance, in particular that "cybercrime cost in 2016 the global economy over $450 billion" [39] (equivalent to our **Rank 4**, but here annualised).

On their side, McAfee and the Centre for Strategic and International Studies[40] "consider that the cost of global cybercrime reached over $1 trillion (… including) monetary loss from cybercrime at approximately $945 billion. Added to this was global spending on cybersecurity, which was expected to exceed $145 billion in 2020"; It is here an amount approaching our **Rank 5** (once again on an annual basis).

Cybersecurity Ventures estimated the worldwide cost of cybercrime at USD 3 trillion in 2015, and at that time predicted a USD 6 trillion for 2021. Their current evaluation announces USD 10.5 trillion annually by 2025, as a result of 15% growth per year, which would reach our **Rank 6.**

Our own quantification work by extrapolation from the French study, concerning the annual cost of cyber prejudices, remains at a more moderate Rank 4, but is closer to Rank 5.

Regardless of their technical ease and of their political likelihood, we shall identify five – not exhaustive – main types of communication and cyber prejudices (it is likely for some to overlap, or for some to be sub-parts in nesting dolls: A < B < C < D) through 5G equipment :

◆ A complete and definitive blockade of 100% of the telecommunication infrastructures of one provider:

• **Case study A** - The prejudice is only for the people's personal telecommunications (professional or private) telephone sets, which will prevent phone call, SMS, MMS, etc.

38- Lloyd's of London and Cyence Report: "Counting The Cost: Cyber Exposure Decoded". Authors George Ng and Trevor Maynard. July 1, 2017. Cyence Inc. applies expertise in data science to the modeling of cyber risks. The company was acquired in 2017 by Guidewire Software, Inc

39- Hiscox Cyber Readiness Report 2017

40-McAfee: "The Hidden Costs of Cybercrim". Authors Zhanna Malekos Smith, Eugenia Lostri and James A. Lewis. 2020.

- **Case study B** - The prejudice also affects IoT, industrial uses (Factory 4.0…), communicating vehicles, etc.

◆ An attack on data, programs and software (owned by people, enterprises, associations, and administrations) by means of the 5G infrastructure provided by one provider :

- **Case study C** (which adds the present data attack to the blocking generated in the cases A and B) - The prejudice resulting from their definitive destruction, encryption or inaccessibility.

- **Case study D** (including case C) - The final prejudice if an intermediate stage adds to case C a provisory undetected falsification of these data, programs and software (able to cause automobile, train or ship accidents, domestic accidents, medical or industrial errors, etc.) in addition to the above destruction, encryption or inaccessibility. A computer worm of the same type as Stuxnet would be representative of this kind of attack, but in this case, on a much larger scale.

◆ Another case study would address the context of large-scale and/or long-lasting telecommunication interception qualifiable as espionage, by means of the 5G infrastructure of a provider. This situation has been seen in the "Hidden costs: estimate of possible data breach by 2030" of the present study report.

The study will retain several hypothesis :

◆ It projects a finalised 5G deployment for countries by 2030, at the end of a roadmap that adopts intermediate steps suggested by the GSMA[41] (47.6% of the French population having adopted 5G in 2025).

◆ It assumes the advent of the "industrie 4.0" with smart factories (so-called fourth industrial revolution), of smart cities/buildings with communicating transports that would be entirely AI-powered and data-driven.
A provider (for instance Huawei) having different market shares from one country to another:

- For France: less than one fifth of the whole 5G equipments market shares (about 15 to 20%). Considering that:
  - Orange (strong leader in France today) previously already chose Nokia and Ericsson, but rejected Huawei's offer (perhaps on the state's recommendation) ;
  - Free, as a result of the French state limitations, stated that it maintained its main supplier relationship with Nokia, without Huawei;
  - SFR already ordered about 50% of its 4G telecommunication equipment deliveries from Huawei, and intended to continue or even to amplify this amount;
  - Bouygues Telecom is in the same situation as SFR.

- Without the French state limitations, however, this percentage could have evolved, especially with the support of Huawei technological and tariff strike force. Indeed, without any state intervention or legal limitation, a floor level could have been estimated at a minimum of 20% of market shares.

- For Germany: about 55% of the whole 5G equipment market share is supplied by Huawei (so triple the French rate). Considering that:
  - Deutsche Telekom has been getting closer to 65% with Huawei
  - Vodafone is similarly oriented towards 55%
  - O2 – Telefonica reached a level of approximately 50%

- For Italy: about 16% of the future 5G equipment market share (the same that the French rate). Considering that :

41-Global System for Mobile Communications Association

- Wind 5G equipments from Chinese suppliers now represent 50% of the total amount (market share in Italy 2019: 13.6%)
- Vodafone now reaches a level of 60% (market share in Italy 2019: 17.46%)
- TIM, Fastweb and Iliad will have no Chinese supplier

- For Portugal, the percentage of Chinese vendor equipment is about 30%.

The presence of three other parameters must be taken into account :

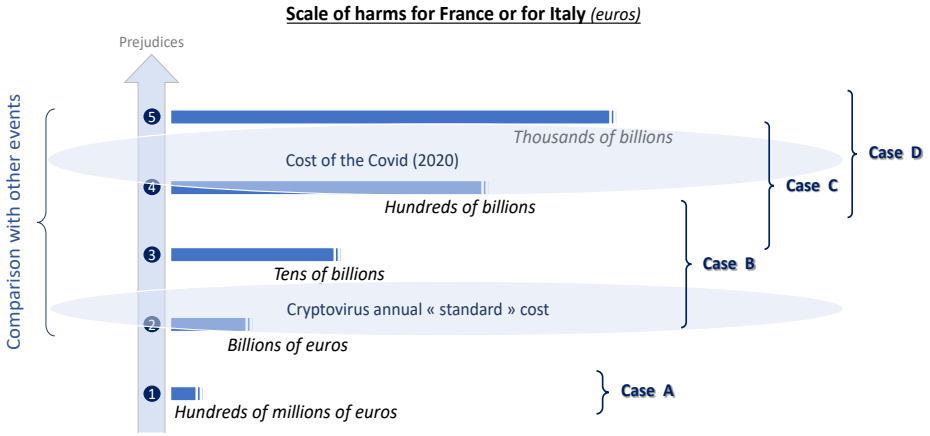
◆ Knowing that this equipment is by their nature intended to communicate with the moving terminals and communicating objects within their reach, during a given period, the percentage of potential targets that would be hit could differ from 20% for France, or 55% for Germany :

- It is, for example, a fact in France that Huawei equipment will be confined to rural and low-industrial areas, which means a customer base smaller than 20%;
- But a potential attack perpetrated over an extended period of time would hit many more mobile users.

◆ These first contaminated targets may be able, in turn, to spread their infection, thanks to their own interconnection capacities. The extent of this amplification cannot yet be accurately estimated.
◆ The future tools of attack (virus …) as well as those of defense – sword and shield – are scarcely imaginable today in their nature and effectiveness.

We will content ourselves with simply relying on our master standard (France) in a comparative process, in order to understand in what proportion each case A, B, C, D would depart from it, above or below.

◆ **Case A** is typical of a rank 1 impact. It appears to be placed lower than the ransomware master, to a significant degree.
◆ **Case B** thus appears to be situated a little bit above the A level – but with a low probability – up to approximately its tenfold – higher likelihood, which does not constitute a definite ceiling. The main reasons are the number of targets reached, far more important than the 4% to 5% of French businesses of which one computer is currently affected by a cryptovirus per year, and the absence of a ransom-type "liberation" and restarting.
◆ **Case C and D** may in turn be significantly above B in terms of nuisance capacity.



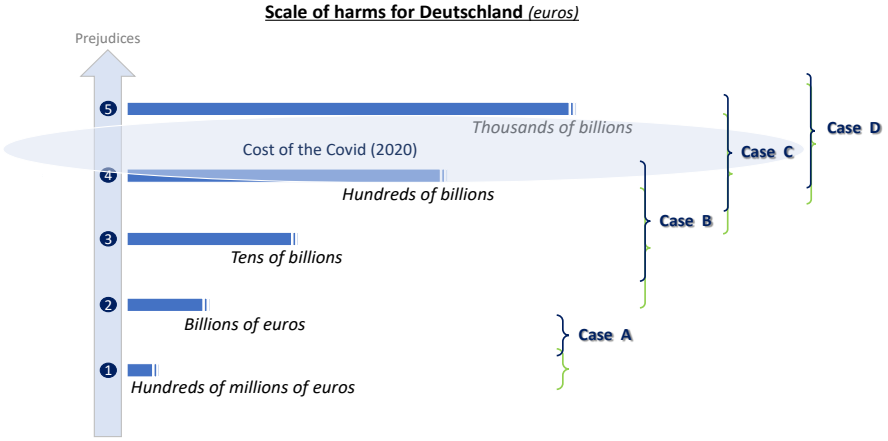
"Scale of harms for France or Italy" illustration: the growth gap (differential of GDP) between these two countries being low, as well as the percentage of market share held by Chinese suppliers (15-20%), it is probable that the damage to their economic systems would be quite similar.

In comparison with the Lloyd's and Cyence study, whose pessimistic scenario's cost for a cyber cloud-service provider interruption was USD 53.05 billion (Rank 3) in the year 2017, our forecasts to a more distant time – 2030 – appear to be compatible. This is especially so given that several 5G specificities, such as the more direct connections between IoTs, will ease uncontrolled propagation on hitherto unreachable targets.

The degree of exposure of Germany is in our example much higher because of the important percentage of market share of Huawei. Consequences would be higher too because of its stronger GDP (or population, used as a reference for the Case A).

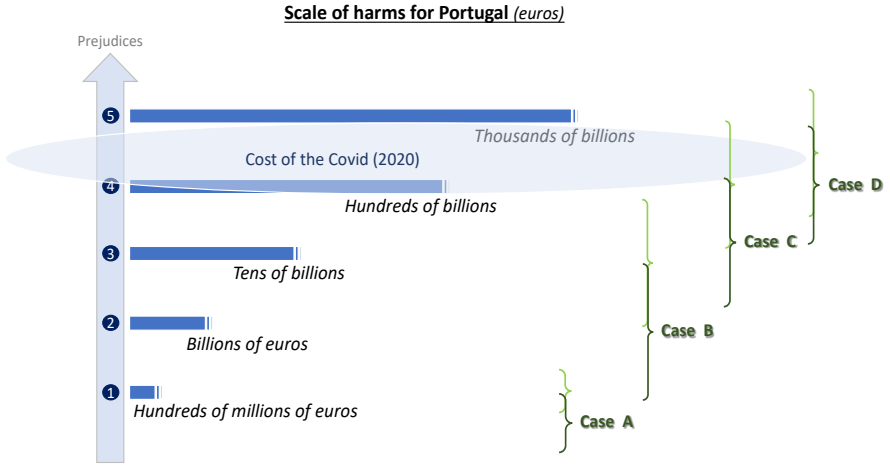
Germany:	3,449,050 million (euro)
France:	2,425,705 million
Italy:	1,789,747 million
Portugal:	213,301 million

This German exposure is also higher because of its ancient and powerful industrialisation, which would make just as many targets (numerically controlled machine tools, steady-state production such as in the chemical industry, etc.). The global level of potential threat is almost quadrupled from France to Germany.



"Scale of harms for Germany" illustration: the green lines in the drawing indicate the French level

The exposure profile of Portugal would, in absolute value, seem at first glance lower, due either to its less important GDP or to its less numerous population. But it is higher in relative terms than for France or Italy, because the market share of Chinese 5G telecommunication providers is about one third of the global Portuguese market.



"Scale of harms for Portugal" illustration: the green lines in the drawing indicate the French level

A first observation is that no German, Italian, Portuguese or French telecommunications operator could afford to pay or compensate the cases C and D, given the amount of money involved.
With any Armageddon technological scenario, another teaching of these screenplays is that there is often no clear limit to the consequences when there was previously no limit to digital interconnections, and no circuit breaker.
Refining in more detail these orders of magnitude would be all the more hazardous because the presence of threshold effects is to be expected, comparable to a dam suddenly bursting after only a bit of water and pressure was added. One can however consider that the dysfunctioning, the shutdown or the pernicious functioning of for example 20% of the telecommunication infrastructures of a country would disrupt many links of any chain, including industrial supply chains, or lead to systemic breakdowns such as in the transport sector or even for smart cities. If the percentage is 55%, threshold effects become highly probable, and the resilience of the global socio-economic system is less certain. A report published by Institut Montaigne evaluating the probability of a "cyber-hurricane" predicted among the causes, "the existence of a "market dominated by a very small number of players. It generates a systemic exposure";[42] this situation, already present in the software and microprocessor industries, takes on greater concreteness when any telecommunications equipment provider becomes a majority supplier on the market.

42- "Cybermenace: avis de tempête". Nov 2018.

BIGS

BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

In June 2019, French authorities adopted a roadmap to accelerate the deployment of 5G networks, and in the same time identified “cybersecurity” as a key challenge that calls for new regulations. The debate on the security of telecom networks is already longstanding in France, dating back to the deployment of 3G networks. However, the interconnected and transnational nature of the infrastructures underpinning 5G networks bring great and unprecedented security challenges.

This country study report for France tries to analyse the French Mobile Telecommunication market and quantifies the hidden costs due to the presence of untrusted vendors in 5G networks. The report is an addendum for France of the BIGS Policy paper “The Hidden Cost of Untrusted Vendors in 5G Networks”. This report details and completes the results presented in this policy paper and quantifies the different hidden costs based on the French context.

The study reports on the current positions of institutional and/or private stakeholders of French mobile telecom market while it identifies and quantifies the country-specific risks associated to 5G. This understanding of the threats includes an initial estimate of the possible costs and prejudices: the cost of security as well as the cost of insecurity. It identifies and weights the financial impact of trust or loss of trust on demand from clients, or on safety recommenda¬tions issued by public authorities.

Overall, the present study reveals a relatively moderate hidden cost levels in France. This could be explained by the cautious posture adopted by France. This posture was materialized late 2019 by a specific law that provides local authorities with the necessary regulation to restrict or prohibit or impose requirements or conditions for the supply, deployment and operation of 5G equipment. This regulation makes it mandatory to get an authorisation from the Prime Minister before rolling-out and operating sensitive equipment for 5G (and future technology, e.g. 6G) networks. It has resulted in a reshape of the French Telecom Landscape, between equipment manufacturers or telecommunications operators. Several of them will have to dismantle or abandon installing some 5G equipment.