BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

The hidden cost of untrusted vendors in 5G networks

STATE OF DISCUSSION AND ESTIMATIONS FOR ITALY

Cefriel
POLITECNICO DI MILANO

Valentina Ferrarese, Enrico Frumento, Gianmarco Panza

COUNTRY STUDY
commissioned by
U.S. Department of State

Brandenburg Institut for Society and Security gGmbH

December 2020 (v1.6)

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 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

List of Figures

List of Tables

1 Executive summary

Discussions about an exclusion of untrusted vendors from building 5G networks or establishing regulatory obstacles, which can be qualified as an exclusion, have occurred and are ongoing in many European countries. Governments, companies, and societies expect a high degree of trustworthiness from those providing the supercritical infrastructure of the future – 5G networks. In addition to the requisite technological skills, the criteria for trustworthiness include an untarnished reputation and an unwavering commitment to respect the laws and rules of the country in which they are providing the network.

The present country study is an addendum for Italy of the BIGS Policy paper. [1] The policy paper reports rationales and more general results about the hidden costs of untrusted vendors in 5G network with limited insights into the relevant countries (Germany, France, Italy, Portugal), apart from a comparison of key indicators. This document details and completes the results presented in the BIGS Policy paper and characterises the various elements in the Italian context.

The three main Italian Mobile Network Operators (MNOs) – TIM, Vodafone and WINDTRE – have begun introducing 5G services to business and consumer customers in the major Italian cities since 2019. Two smaller MNOs, Iliad and Fastweb, are aiming to launch services early in 2021. This ongoing deployment process leverages a complex supply chain for novel network technologies.

In 2019, the Parliamentary Committee for the Security of the Republic (COPASIR), expressed concerns in relation to Huawei in its reserved report. [2] This ultimately led to the advice to exclude Huawei from the development of 5G networks in Italy. The document is secreted, but according to the press, it is one of the early reports that clearly expressed concerns against "untrusted" operators, given that a clear definition of "untrusted vendor" does not yet exists in the Italian legislation, the Italian legislation, however, prefers to use the term extra-EU vendor.

The main vendors for 4G and 5G network equipment present in Italy are Huawei, Nokia, Ericsson and ZTE. The Chinese (extra-EU) vendors are still considered untrusted. This is a significant issue because Italy is one of the EU countries with a 4G infrastructure where greater than 50% of components come from untrusted vendors, and the first phase of 5G rollout is based on 4G infrastructure. Particularly low profit margins in the Italian telecoms market are driving MNOs to mutually share infrastructure by partnerships (e.g. towers and backhauling) and opt for a multi-vendor 5G Radio Access Network (RAN) when equipment, also from untrusted vendors, has already been installed. Indeed, the costs of subsequent rip and replace – at least of sensitive 'core' network components – may be prohibitive (in other words, equipment from untrusted vendors in the core is not actually an option for the Italian MNOs). In addition, the offerings from untrusted vendors are oddly cheap, and therefore highly appealing for addressing cost effectiveness. In such a scenario, it is critical to estimate and disseminate the hidden costs associated with the adoption of technologies from untrusted vendors. The aim is to raise the level of awareness among MNOs to facilitate them making more informed decisions when building 5G networks, upon which the future of the economy and society heavily depend.

The Italian government has ambitions to host the first fully realised 5G network of the larger European countries. Italy was the first EU country to auction 5G spectrum to MNOs (this ended on 2 October 2018). Italy's unusual telecoms market structure – 'wholesale' – may help to reduce future hidden costs by centralising control and oversight of access and transport (backhaul) communications in one actor whose identification is not yet finalised.

However, Italy's legislative framework for the introduction and management of secure 5G infrastructure is not yet fully finalised. Italy is applying the EU Toolbox and its own Golden Power frameworks, with the latter extended to include the 5G networks and operators (Article 1-bis of L 21/2012, special powers relating to broadband electronic telecommunications networks with 5G technology).

Additionally, Italian MNOs must abide by plans for the National Cybersecurity Perimeter (NCP) and the decree of the Minister of Economic Development, which establishes the creation of National Evaluation and Certification Centre (Centro di Valutazione e Certificazione Nazionale – CVCN- L. 105/2019 and 133/2019) with the aim of mitigating cyber risk. The CVCN is called upon to assess the supplies of specific categories of ICT goods, systems, and services that the perimeter subjects intend to acquire to use on networks, systems and services included in the perimeter. The CVCN will perform preliminary checks and impose conditions and further tests on hardware and software to carry out its verification and validation activities.

In 2019, the Italian Parliamentary Committee for the Security of the Republic (COPASIR) advised the Italian government to exclude Huawei from Italian 5G networks in its reserved report. Despite this, the government did not make a definite decision. However, with the development of the NCP, the government has now adopted a decree allowing untrusted vendors to develop 5G infrastructure so long as they abide by stipulated regulations.

In addition to the obvious costs that incur when a supercritical 5G network is sabotaged, there are also less visible or hidden costs that incur when the confidentiality and integrity of the network and its data is being compromised. These costs are hidden because they occur either later in time or because they are borne by people or institutions other than by those who decide upon the architecture (and its parts) of the 5G network.

As of the end of December 2020, this country study outlines and roughly quantifies the hidden costs in the Italian context:

- Costs of test centre to detect and evaluate malicious bugs in the frequent software updates of a 5G network. Based on estimates of the size of the market and the scale of untrusted vendors' role in each market, we estimate Italy's National Test Centre could cost EUR 40 million per year.
- Costs of regulation. The validation costs (though not entirely for the testing ones) are always covered by the government and the application costs are due for both trusted and untrusted vendors. In the case of untrusted vendors, the validation might take longer than usual. Since the CVCN is not yet active, there is no data on its averaged performances, but we believe a realistic hypothesis is that the validation would be 50% longer than usual for untrusted devices, because of the general need to perform tests that are more scrupulous.

- Costs of data breaches. We estimate annual costs of data breaches of around EUR 580 million by 2024. Whilst surprisingly low, this is because data breaches occurring over untrusted 5G bearer networks are likely to form a low proportion of overall breaches in the country. Interviews with MNOs and our analysis confirmed that the percentage of data in transit over untrusted technologies on the 5G network is likely to be small, providing as little as 8.9% of total capacity by 2024, if the current market share is confirmed (additionally, full 5G network coverage is expected no earlier than 2024, with about 70% of mobile traffic still over 2G-4G).
- Costs of shift of demand. We estimate more than half, or EUR 1.342 billion, of revenue from commercial customers in the telecommunications market may be at stake by shifting to trusted networks. Italy's 2020 market (EUR 31.576 billion) was less than half the size of Germany's, with only a slightly greater proportion of revenue generated through mobile telecommunications services (47.41% compared to 43.97%), and a lower proportion of business users (17.94%) as a percentage of total revenues.
- The presence of untrusted vendors in a future 5G telecommunication network might force the government to invest in a redundant infrastructure that is fully controlled by the Italian state; we estimate a gross value of EUR 700 million.
- Costs of rip and replace. We expect costs of around EUR 600 million, without a significant delay in the development of 5G infrastructure.

Overall, we show in this country study that the total societal costs, i.e. including externalities, are higher over time than the potential savings that arise for mobile network operators when they use non-trusted network technology to deploy 5G. Ultimately, this evidence should support decision-makers to assign priority to the realisation of trustworthy 5G networks.

2 Introduction

Italy has spent resources to strategically be at the forefront of the 5G competition since the early phases of 5G. Italy is one of the first movers deploying a next-generation network, despite the COVID-19 difficulties. In 2019, A.D. Little ranked Italy as one of the leading big economies most investing in 5G. [3] For the present country study, the authors interviewed representatives belonging to the major telecom operators, insurance companies, academia, and regulatory bodies. Other sources come from authoritative international reports and studies, updated until December 2020.

3 The Italian legislative framework

The Italian government is keen to make Italy a world leader in 5G to address the digital divide and complete the digital transformation of key sectors (e.g. manufacturing, health, and education), the Public Administration (PA) and Italian society. The Italian regulatory bodies are working with the government and industry to make this happen. Since 2018, the government has been investigating the security impact of 5G as a strategic service and nationwide infrastructure with a regulatory body. The legislative framework is composed of a combination of European indications (e.g. European Toolbox) and national integrations. The Italian set of legislation is composed of three elements: the European

Toolbox, the Golden Power (GP) indications that have been extended to include 5G, and the National Cybersecurity Perimeter (NCP). The main characteristics are as follows.

- **EU Toolbox.** Published on January 29, 2020 by the NIS Cooperation Group [4] [5] and valid across the entire European Union. It defines horizontal and vertical risk mitigation measures distributed across nine key risk indicators. This is a European cyber risk mitigation policy which applies to all actors implementing 5G services (i.e. MNOs and private 5G networks). [1]
- **Golden Power (GP).** GP is a national regulation that defines rules for acquirers of technologies from non-European vendors. The legislation was extended to include 5G networks and operators (Article 1-bis of L 21/2012, special powers relating to broadband electronic telecommunications networks with 5G technology). This is an Italian set of obligations with specific extensions for 5G that applies to all the relevant actors for the national security (e.g. MNOs, public bodies, critical infrastructure). The law set three types of countermeasures:
    - "Restrictions for high-risk suppliers". Under the GP law, the government receives notifications in case MNOs deploy 5G equipment or services sourced from extra-EU suppliers. An inter-ministerial coordination group advises the government about the option of vetoing the contracts (based on technical analysis) or imposing security measures. [5, p. 18] An example of additional security measures is, in the case of devices from non-EU suppliers, the disabling of the remote controlling interfaces by default and the request to operate locally.
    - "Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies and avoiding dependency on high-risk suppliers". In contexts where the GP applies, MNOs are requested to introduce both "vertical" (the use of different supplier systems in the hardware, virtualisation, and application layers) and "horizontal" (the use of different providers of software solutions, at application layer) diversifications. [5, p. 22] According to our interviews, most MNOs have already implemented geographic diversification to minimise risk by segmenting geographic areas (in other words, the area controlled by the network equipment of a single vendor is limited to contain the impact of a potential security incident).
    - "Ensuring secure 5G network management, operation and monitoring". The baseline requirements to address this technical measure are included in the Decree of the Ministry of Economic Development "Security and integrity measures of electronic communication networks and notification of significant incidents" of the 12 December 2018 (secondary legislation), Article 4(1)(h) and (i). Within the application of the GP, MNOs are not allowed to outsource the Network Operation Centre (NOC) and are requested to attain a high level of autonomy in running their networks [5, p. 34].

[1] NIS regularly monitors the evolution of nine risks [4], the topmost of which are "R1: Misconfiguration of networks", "R2: Lack of access controls" and, "R5: State interference through 5G supply chain". In average across months the less mitigated risk is R5.

- **National Cybersecurity Perimeter**.[2] The NCP aims to ensure a high level of security of the networks, information systems and IT services within the public administration, private and public entities, and operators that have an office within the national perimeter. The legislation applies to 5G MNOs and influences the security of 5G networks. The NCP legislation will be completed by application decrees still under discussion. The legislation demands that all private and public operators included within the NCP test the processes, technologies and software in a National Evaluation and Certification Centre (Centro di Valutazione e Certificazione Nazionale – CVCN- L. 105/2019 and 133/2019). MNOs sustain application costs. The CVCN will play the role of risk assessment and verification of the security conditions and absence of known ICT infrastructure vulnerabilities whenever a public or private operator adopts goods, ICT services, informational systems or network equipment that falls into the NCP.[3] It is, however, important to underline its role of validation and evaluation, and not certification of products, in advance of their installation.

One peculiar aspect of the Italian legislation is the absence of a shared concept of untrusted devices. As reported by the press [6] at the presentation of the recent Italian I-COM (Institute for Competitiveness) report on 5G [7], the General Secretary of Palazzo Chigi Roberto Chieppa stated: "*Today there is no certainty on the parameters on the basis of which a vendor can be identified as a high-risk vendor (i.e. as the US has defined the Chinese Huawei). It is still necessary to decide if this concept should be left only to a strictly technological evaluation (in SW and HW, horizontally and vertically), or if other elements, such as those indicated in the COPASIR report of more economic and strategic natures, or even other aspects related to international relations (e.g. with NATO allies and China) that may derive indirectly, should be included in this evaluation*". This point of view is confirmed by the interviewed MNOs, among which there is no clear agreement on how or methodology through which to calculate the cyber risk of untrusted vendors in general (and therefore, the resulting costs).

In January 2021, it was reported that the EU is working on a cyber-certification of 5G. In the workstream of the NIS Cooperation Group on 5G, a subgroup "Standardization and Certification" has been proposed for the creation of an EU system on 5G. Accordingly, MiSE (Ministero dello Sviluppo Economico – the Ministry for Economic Development) announced at the beginning of 2021 [8] that it is working on a cyber certification, specifying that ENISA should provide such a certification scheme. In the updated EU cybersecurity strategy presented on 16th December 2020, the member countries are "encouraged" to fully apply the EU toolbox by the second semester of 2021 [9]. The action-lines of the strategy have a wide scope, as they address three objective groups: (i) resiliency, technology sovereignty and leadership, (ii) development of the prevention, deferring and mitigation capacities of the security operations against cyberattacks, and (iii) promotion of a global international and open cybersecurity space cooperation.

[2] DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 30 luglio 2020, n. 131; in G.U. del 21 ottobre 2020, n. 261. Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. (20G00150). Vigente al: 5-11-2020

[3] Funding will be inserted in the budget law 2021.

4 Current state of the market in Italy

According to a recent document commissioned by the government, [10] the Italian market has some peculiar aspects of interest for the present country study.

- Wholesale network
- Non-Stand-Alone (NSA) 5G networks as initial choice
- O-RAN implementation plans
- The evolution of private 5G networks
- High competitiveness of the Italian telecom market with low price Gb/persona

In Italy, there are three main MNOs shareholders: TIM, Vodafone and WINDTRE (a result of the merging of WIND and H3G) and two smaller ones, namely Fastweb and Iliad. Another, Linkem, has a minor market share. There is also the peculiar operator EOLO, which will mainly use the Fixed Wireless Access (FWA) methodology because of its unique market positioning (connecting remote, alpine, and rural areas). All of them, apart from EOLO, participated in the auction for the 5G spectrum and acquired licenses for frequency slots in the bands sub-1 GHz, sub-6 GHz and above 24 GHz (i.e. MMW). Notably, Italy was the first EU Country to assign slots in all such frequency bands. The result of the auction (concluded the 2nd of October 2018) is as follows in Table 1.

Table 1: Italian MNO and assigned frequencies for 5G. (*) Iliad was granted 10 MHz in the 700 MHz at the basic opening price (as a newcomer).

Band	*Fastweb*	*Iliad**	*TIM*	*Vodafone*	*WINDTRE*
700 MHz		2x10 MHz	2x10 MHz	2x10 MHz	
3700 MHz		20 MHz	80 MHz	80 MHz	20 MHz
26 GHz	200 MHz	200 MHz	200 MHz	200 MHz	200 MHz

The main MNOs have already started deploying 5G networks.

- TIM and Vodafone have launched business and consumer services in most of the main Italian cities. Furthermore, Vodafone is extending coverage to suburban areas around Milan, while TIM is covering Saint Marine and realising novel services enabled by 5G in southern Italy. TIM and Vodafone have also agreed to share network assets to cover 100 other cities and several industrial and tourist areas by the end of 2021 with the creation of the company INWIT, owning more than 22,000 towers.
- WINDTRE is providing 5G services in the main Italian cities and plans to target 77 cities by the end of 2021.
- Iliad and Fastweb are working on 5G network deployment, though at a slower pace. Specifically, Fastweb has announced the launch of mass services at the beginning of 2021, pushing the FWA (Fixed Wireless Access) technology, an experiment around which it is currently running in the city of Bolzano. Fastweb and Linkem are sharing their assets to provide FWA (up to 1 Gb/s) to hundreds of localities, also covering several rural areas currently part of the digital divide.

4.1 Wholesale model

One peculiar aspect of the Italian market is the potential adoption of the wholesale model for 5G for the fixed (mainly fibre) access and transport. The target should be carried out in

two steps by company integration, involving the incumbent TIM and other network providers. Currently, this model is still in its infancy and needs to be approved by the EU commission as efficient and sustainable, guaranteeing neutrality and future investments. Indeed, the wholesale model is already widely used for the national fibre connection access and backbone by OpenFiber. [10] This approach is important in terms of hidden costs and risks because it centralises responsibility for risk management to a single actor. The wholesale model also applies on a private level, through the sharing of infrastructures between MNOs, as a common means to reduce costs.

Theoretically, the central actor operating the wholesale model could be OpenFiber, who built most of the rural and currently low-market profile fibre network (a separate fibre network also exists, owned by TIM and Fastweb). Another actor is the towers company INWIT (Infrastrutture Wireless Italiane), newly formed as a private venture from the fusion of TIM and Vodafone assets. In addition to hosting operators on its towers, INWIT is building its own DAS (Distributed Antenna System) infrastructures to allow widespread coverage of crowded open spaces or large closed spaces intended for commercial activities, leisure, and sport (stadiums) or health infrastructure (hospitals). The wholesale model and its leadership are nowadays at the centre of political discussion, with both technical and business matters on the table.

4.2 Non-standalone (NSA) 5G networks

Italy is one of the 15 EU countries with more than 50% of 4G infrastructure still based on untrusted (where not differently stated we mean for example Chinese products) or in general, extra-EU vendors. The presence of that kind of equipment has been confirmed by multiple-MNOs in critical areas (i.e. big cities or key industrial districts), as well as in lowly populated or secondary economic areas. The distribution of untrusted devices across Italy varies among MNOs. As Italy was one of the first EU countries to begin deployment of 5G networks (already in 2019), the main MNOs initially leveraged the existing 4G infrastructure to build the NSA (Non-standalone) option of 5G Release 15. [10] Progressing from this, 5G SA (standalone) is already being deployed. One early consequence of the government's obligations and the EU Toolbox is that the dependency of 5G infrastructure on untrusted equipment vendors is generally lower than 4G. Furthermore, the selection of core network technology, where the systems' intelligence resides, has been made in favour of trusted vendors only, both for having best-of-breed technology and for security reasons. However, migration to 5G SA is unlikely to be complete before 2022. Interviewed experts underlined that the domino effect on 4G will be considered a hidden cost of a rip and replace, following the ban of a specific provider, and no full evaluations exist yet.

4.3 O-RAN implementation plans

From a technological point of view, none of the Italian MNOs will deploy in the short- and mid-terms O-RAN compatible equipment. However, as also demonstrated by experimentation in some EU countries (e.g. Vodafone in Ireland and Telefonica in Germany [11]), key figures in academia and industry consider O-RAN as a viable and likely approach in Italy as well (not only for 5G and beyond, but also for 3G and 4G, due to its flexibility,

cost-effectiveness, and open nature). Indeed, an open and more modular architecture increases competitiveness and allows for a deeper security risk analysis and investigation. Higher competitiveness entails reduced dependence on a small set of vendors, as well as lower costs.

A report of ABI Research [12] estimates the Open RAN market to be 75% of the global market in 2030, with total radio unit spending for outdoor macro-networks of EUR 56.8 billion, with 15.7 million units sold. Simultaneously, the indoor enterprise Open RAN segment for small cells will reach EUR 32.5 billion in 2030, with 205.5 million network units sold.

4.4 Evolution of the private 5G networks

Release 16 of 5G standard adds support for unlicensed spectrum, known as NR-U (NR-Unlicensed).

5G NR-U introduces unlicensed spectrum bands (e.g. 5-6 GHz), and includes the License Assisted Access (LAA). LAA lets operators aggregate unlicensed spectrum with an anchor channel in the licensed spectrum for multi-gigabit speeds. Like LAA used with 4G, it is possible to use unlicensed frequencies in a defined geofence for the local connectivity, and bridge to a licensed frequency the geographic area connections. Release 16 also provides the standalone NR-U mode, which works without the anchor in (i.e. without need for) licensed spectrum.

Release 16 enables a new category of services, ultra-reliable low latency (eURLLC). Ultra-reliable low latency communications are used for mission-critical applications like industrial IoT, providing up to 99.999% reliability with millisecond-order latency. This means that it is possible to deploy a cellular system without an MNO's involvement (i.e. the only granted licensee), as a private 5G network, also named Non-Public Networks (NPN).

NPNs are critical enablers for the transition to 5G of connectivity solutions using reliable wired or dedicated wireless technologies (less often). An NPN offers 5G connectivity inside the logical perimeter of the premise and is bridged to the public network with a dedicated firewall.

The applications of NPN are growing. According to ABI Research, [13] the revenue generated by private cellular networks will be around USD 64 billion by 2030, with main sectors being Industry 4.0, utilities, and logistics. In Germany, since November 2019 [14], it has been possible to license the 100 Mhz spectrum for local and private networks. BMW, Bosch, Volkswagen, BASF, and Lufthansa have applied [15]. At the beginning of April 2020, according to the Wall Street Journal, [16] 33 enterprises in Germany had acquired the rights for the 100 Mhz spectrum.

In Italy, the MiSE (Ministero dello Sviluppo Economico) granted the 100 Mhz bandwidth for trial purposes only. At the time of writing, three trials are running, all using extra-EU vendors: Milan (Vodafone with Huawei), Aquila and Prato (WindTre-OpenFibre with ZTE), Bari and Matera (TIM-Fastweb with Huawei).

5G NPN allows the realisation of private cellular networks, without being tied to an MNO for licensed spectrum and enabling the ability to choose the preferred devices (e.g. using

other criteria like the economic convenience). This context is less regulated than the MNOs networks and represents a possible area of risk connected to the presence of untrusted devices in IPR-intensive implants.

As already discussed in Section 3, the Italian legislation that applies to 5G has three pillars: the European Toolbox, the Golden Power extended to include 5G, and the National Cybersecurity Perimeter. The EU toolbox and GP do not necessarily apply to private networks, unless they form part of an actor's infrastructure under the control of GP. Additionally, the focus of NCP is the critical infrastructure and services, and it is not yet clear to which actors the CVCN applies in the case of NPN. The involvement of extra-EU vendors in the Italian trials shows that NPN is a promising area for their commercial interests.

4.5 Competitiveness of the Italian telecom market

Italy has a highly competitive telecom market compared to other European countries. This factor hampers the option for MNOs to afford expensive mitigations, if not mandatory or required by the legislative framework. As reported by CNIT, [17] the cost (resulting from auction) per MHz (MEUR/MHz) in the 3400-3800 MHz spectrum for Italy is the highest in Europe (22) and approximately twice the cost of Germany, the second most expensive country. (14) The average yearly drop of revenue per Gb in Italy is around 43%, while in Europe it is approximately 20%: with EUR 10 in Italy, a customer gets an average of 9.3 Gb in traffic, while in Europe, the mean, excluding Italy, is only 2.3 Gb [10].

5 Current state of debate in Italy

In 2019, the Parliamentary Committee for the Security of the Republic (COPASIR), expressed concerns in relation to Huawei in its reserved report. [2] This ultimately led to the advice to exclude Huawei from the development of 5G networks in Italy. The document is secreted, but according to the press, it is one of the early reports that clearly expressed concerns against "untrusted" operators, given that, as anticipated in Section 3, a clear definition of "untrusted vendor" does not yet exists in the Italian legislation, the Italian legislation, however, prefers to use the term extra-EU vendor. As well as this, the study reports a rough estimation for a rip and replace extended to all the subjects of the GP: gross estimation of the total costs is around EUR 600 million, without a significant delay in the development of new technology. [18] [19] Despite this warning, the government took no further action. The assumption at the time was that Italy's GP law was enough to protect the country from the risks identified by COPASIR. However, only the government can activate the GP regulation on a case-by-case basis. Therefore, unless the government invokes it in the specific case of an "untrusted" operator in the development of 5G networks, Italy is not entirely protected from the threats identified by COPASIR. [19] Nowadays the definition of the national cybersecurity perimeter and the incoming launch on the market of 5G services reopened the discussion. According to press, in March 2020, COPASIR further requested that the Office of the Prime Minister adopt clearer regulations and plan to secure the development of 5G networks in Italy [20]. To this, the European Toolbox does not fully address the relevant issues, because it specifically

concentrates on mitigation of cyber risks arising from compromising, tampering or back-dooring of the RAN (Radio Access Network) devices (as already mentioned, the core of the 5G network is built on technology by European vendors, Ericsson and Nokia, entirely for the Italian MNOs and almost completely for the MNOs of the other EU member countries). The Italian situation is also described by the I-COM study entitled "The 5G to relaunch Italy in safety" ("Il 5G per rilanciare l'Italia in sicurezza") [21]. I-COM reports the difficult European situation on 5G and underlines the imbalance between offering, competitiveness, and applications: "in the old continent, in fact, there are only 779 users connected to 5G per 100,000 inhabitants". According to the report, Italy is ranked third in the European Union's 5G development agenda.

Nonetheless, as notified by the press, [19] [22] on 7th of August 2020, the Italian government adopted a decree on 5G intended to increase the security of its rollout. The decree regulates the flow of mandatory information about extra-EU apparatuses setups and uses. The decree incentivises diversification and impose fines for providers who do not comply with these rules. Such a decree intent is to allow untrusted vendors to participate to the development of 5G networks if they abide by the above regulations.

With the already cited NCP, the government aims to ensure a high level of security of 5G networks and clarify these apparent contradictions with coherent legislation.

5.1 Insurance situation in Italy

In its SONAR Insurance report of 2019, SwissRe Institute identifies 5G as one of the key challenges for the insurance and reinsurance industry. [23] One of the main characteristics of 5G, from the insurance point of view, is its ability to enable digital analytics capable of rapid analysis of massive amounts of unstructured data. The combination of more data and better analytics can lead to better insurability of previously difficult-to-price products, and to new capabilities in fraud detection. The loss potential of these risks is currently difficult to estimate, but they may have a major business impact on the insurance industry. The SwissRe study also underlines the risk of "built-in hard- or software backdoors" and the possibility of concentration of risk due to the increasing focus of the 5G market around a few firms.

In the case of 5G, the insured subjects can be either MNOs or users. For the insurability of MNOs, the presence of risky or untrusted vendors in the 5G network represents, for the insurance broker, a silent cyber risk.[4] According to the interviewed experts, the compromising of a 5G network could manifest as a warlike scenario where limitations apply (e.g. the U.S. TRIA Act). However, a mitigation instrument like the like U.S. TRIA, despite its controversial applications, [24] does not exist in Italy.[5] When using untrusted technology, a public network operator or a private network industrial operator in the case

[4] A silent cyber risk is the potential financial loss incurred from cyber-attacks due to silent coverage within insurance policies that were not designed to cover cyber risk [59]

[5] Italian insurance market self-regulated itself. Nowadays almost any insurance includes specific exclusion clauses on cyber war or cyber terrorism, to limit applicability. One main insurance company in Italy defines an act of War and Terrorism as "War, terrorism (except Cyber Terrorism), invasion, military action (with or without declaration of war), civil war, mutiny, popular or military revolt, insurrection, rebellion or revolution, military power or usurpation of power or any action taken to obstruct or defend against any of these events." Like in US (see clause of Mendelez for the NotPetya attack [61]) are unclear.

of private 5G network, has a higher risk of successful cyberattacks. The typical AAA process (Authentication, Authorisation and Accounting) is limited because of lack of transparency or trust at some point in the technological supply chain or the service logic layers. In general, therefore, 5G network cyberattacks cause high damages that need to be borne either by the network operator or by their customers. One common way to deal with this risk is to buy an insurance plan. However, typically in Italian insurance policy texts, one of the triggers for the activation is that the products sold to customers (for example, insured telco that provides 5G equipment to industries) are subject to an order from an authority that decides the withdrawal from the market (for whatever reason). Nonetheless, very often the policies specify that the order to change must be linked to the risk of damage to property or persons, excluding the privacy risks. Therefore, in general the insurance companies in Italy today require a case-by-case analysis because in some cases, the recall policies are beyond their scope. In the insurance world, product recall covers only some specific costs, which are those for withdrawal from the market (e.g. transport, storage, and substitution) and, if specific options are present in the insurance contract, the costs of disassembly and reassembly of replacement equipment. The insurance, however, does not cover consequential damages (downtime) or the value of the equipment itself. Given the exclusion of privacy risks and the predominant attention to physical damage risks, the security of Operational Technology (OT), has a special role. OT does not only imply cyber consequences but also safety (e.g. risks of explosions) and production stops (e.g. economic damages). This is a grey area for the insurance market and no clear pricing is yet defined. However, the industrial sector is one of the sectors most impacted by the 5G evolution. One aspect of interest for insurance and risk measurement is that O-RAN allows deeper and more detailed investigations (i.e. it eases the attribution of responsibility) in the case of a security problem (i.e. thanks to its accountable and modular architecture).

5.2 Civil protection

Italy is one of the European countries with the most developed civil protection and emergency infrastructure. The country presents many risks, both of the natural kind (seismic, volcanic, hydrogeological, hydraulic, etc.) and of the anthropic kind (chemical, industrial, transport, etc.), inland (forest fires, etc.) and on the coasts or in the open sea (tsunamis, maritime accidents, etc.). Hence there is a relevant number of redundant operating emergency networks (using UHF/VHF, radio, TETRA etc.) which have historically responded better to its individual operating conditions. The coordination of Italy is, at the national level, through the National Civil Protection "system". However, different subjects are collaborating (at local, regional, and national levels) with the coordination bodies (National Civil Protection Department, Regions, Prefectures and Municipalities) and with national operational structures (Firefighter, Armed Forces, Police Forces, Health System, Italian Red Cross, etc.) [25] or local operational brigades (Municipal civil protection associations, ecologist associations, etc.). Although this emergency response system is very flexible and timely, it varies in communications and data exchange formats.

According to interviewed stakeholders, the discussion about how to migrate these structures to 5G has not yet begun and they have not produced public estimations. Some

specific experiences have been undertaken with 5G, such as the "5G connected ambulance of the Italian Red Cross". [26]

6 Alleged costs of market intervention by banning untrusted vendors

The Italian government has, since its early stages, recognised 5G as a critical technology and an opportunity to bridge the gap with other European countries for the European agenda for 2025. The previously cited analysis of I-COM [21] provides an estimation of the investments needed to realise a full 5G network in Italy. The document estimates the additional costs of the exclusion of extra-EU vendors as within a range of EUR 4 to 5 billion. However, these values come from the data presented by "Asso telecomunicazioni" in April 2019. [6]

A more recent Oxford Economics [27] study (June 2020), sponsored by Huawei, describes the Italian situation and projections. The document estimates that the global recession, including the impact of the first wave of the coronavirus, will leave a painful scar on Italy, with the economy shrinking by 9% in 2020. In the current recession context and subsequent recovery, a competitive stable, and trusted market for 5G infrastructure would help to maximise technological innovation and growth in Italy. The estimated economic turnover for 5G services and associated activities in Italy is EUR 15.7 billion in GDP with job creation of around 186,830 units. The Oxford Economics study also underlines that restrictions of the competition will have adverse economic impacts. The Oxford model suggests that restricting a major participant (namely Huawei) could increase the cost of building the 5G network by EUR 282 million per year over the next decade (19% of baseline costs) in a central cost scenario. Due to this price increase, 6.9 million people (12% of the population) who would have otherwise had access to the 5G network could be left without in 2023. The document also claims that restricting competition in the network infrastructure market may significantly reduce economic growth in Italy over the next 15 years, with a consequent reduction of the GDP in 2035 of EUR 4.7 billion.

However, considering the Italians' up-to-date indicators, the Oxford Economics study, commissioned by Huawei, an extra-EU vendor, have potentially overlooked some elements. The pandemic affected the Italian economy and stressed its telecommunication infrastructure. AGCOM [28] in July 2020 reports, for the first half of 2020, a traffic increment of 44%, which the existing MNOs infrastructures managed fully, and an economic recession of only 5.7%. Moreover, the whole ICT sector is expected to decrease by only 2% by the end of 2020 [29] and return to growth in 2021 (3.4%) and 2022 (3.3%), thanks to the demand for products and digital services, supported by 5G. 5G is foreseen in Italy to be a revolution in terms of enlarged ecosystems and novel business models. The MNOs are increasingly becoming more than connectivity providers, migrating their portfolios and revenues towards high-value ICT services. Along the same lines, the report "Harnessing the 5G Consumer Potential" [30] by Ericsson Consumer Lab, estimates a global MNOs revenue increase of up to USD 133 billion by 2030, mainly because of digital

[6] Data presented by Asso telecomunicazioni-Asstel during the reporting to the Italian Parlament in April 2019, on the matters of 5G, Big Data and radio waves.

services. Another element that the Oxford Economic study did not consider is the Recovery Fund (not fully defined at its release date). The Italian government already announced the allocation of a consistent contribution to boost the digital transformation agenda and provide broadband access (including mobile, i.e. 5G) to reduce the national digital divide.

Moreover, the government already confirmed the pre-COVID national roadmap for the new generation of cellular systems. This confirmation is a sign of trust that the announced European restrictions for extra-EU manufacturers will not reduce MNOs' market share and economic forecasts. All the interviewed MNOs share this confidence, despite possible exclusions of specific suppliers: the application of requirements/countermeasures derived from combined effects of the EU Toolbox, GP (when needed) and NCP are a safeguard against the presence of untrusted vendors. This is completed by ready-made plans to mitigate the impact of an exclusion of the extra-EU vendors.

According to the comparative report among Europe, Australia, and the US, published by the Copenhagen-based Strand Consult in November 2020, [31] entirely restricting Huawei and ZTE from Australian and US networks has not increased prices or delayed rollouts of 5G. The study forecast a similar impact in Europe: "*restrictions did not result in price increases in the US or Australia and are unlikely to negatively impact Europe as well because Huawei and ZTE's footprint in Europe is but 6% of the world's total outlay*". Specifically for EU countries, the report estimates that a replacement of Chinese vendors' equipment would cost European MNOs about EUR 3.5 billion, significantly lower than the values reported by Oxford Economics.

According to the interviewed Italian MNOs, the complete switch to trusted EU vendors (e.g. Ericsson or Nokia), is less expensive than expected in 2019. Interviewed stakeholders also reported that the technological and offering gaps among European and extra-EU vendors is nowadays rapidly reducing, shifting the balance towards European vendors amid the risks and economic/technical advantages.

The study "5G action plan for Europe" by Analysys Mason [32] estimates the economic impacts of 5G transformation on utilities, arts, healthcare, and education among others once the first 5G roadmap is completed (i.e. almost full coverage foreseen by 2025). The study focuses on both consumers and businesses aspects. The estimated costs of a full 5G deployment in Europe is EUR 46 billion, with a considerable cost-benefits ratio of 4.5. For Italy, the cost of the 5G rollout is estimated at EUR 6.6 billion with a rate of 2.2.

Combining the values reported by the studies published following the Oxford Economics report, the additional cost of a full 5G deployment with the hypothetical restriction to EU (trusted) vendors is, for the whole of Europe, less than 8% (i.e. EUR 3.5 over 46 billion).

The last DESI (Digital Economy and Society Index) report on telecoms chapters [33] shows that it is reasonable to keep the same averaged percentage for Italy: Italy being one of the first countries to begin the 5G rollout, its economic indicators are aligned with those of the more digitally advanced EU nations. These values are lower than those presented in the Oxford Economics report, but also lower than the projections made in 2019. [21] Of course, this is also a result of the long-term changes induced by the global pandemic: the

COVID-19 pandemic hit hard Italy and its effects, combined with a fast-evolving market, means the scenarios progress faster.

7 Obvious costs of malicious vendors

As presented in the Policy Paper, [1] the most obvious costs of untrusted vendors occur when the network is being used to sabotage an entire economy. For this "Armageddon Scenario", the effect of such an act of sabotage on the Italian gross domestic product (GDP) would probably, at any rate, be comparable to that of a few days' general strike or a full lock-down during a pandemic. Based upon recent calculations conducted by the BankItalia [34] to evaluate the effects of a nation-wide lockdown due to COVID-19 pandemic, each lost working week corresponds to 0.5 percentage point of GDP. Taking the Italian 2019 GDP of EUR 2450 billion [35] as a basis, an interruption of working life for three days would translate into an absolute amount of about EUR 5.25 billion, without taking into consideration cascading and other second-round effects (e.g. the costs of a then unavoidable and precipitous post-incident, reactive rip and replace). Most probably, getting the communication network fully fixed within three days would be a naive pipe dream.

While the blackout scenario is unlikely (disregarding maybe a one-time shot in an international confrontation), a more realistic one might be a more furtive pouring of sand into the gearbox, over a longer time, and thus thwarting the Italian industry communication infrastructure, and thus the economy. Such a gradual obstruction could either target the economy or be aimed at sectors of strategic importance, for example, the Italian manufacturing sector with its industry 4.0 production.

8 Hidden costs of untrusted vendors

The following part of the report details the hidden costs of remaining with untrusted vendors for Italy. The following sections start from the conclusions drawn in the BIGS Policy paper [1] and provide details for the Italian situation. As reported in the policy paper, the hidden costs can be divided into lifecycle costs and external costs (see Table 2). Some costs are both external and occur later in the lifecycle.

Table 2 - Nature of hidden cost categories – external and lifecycle costs (source [1]).

Cost Bearer MNO	Cost Category		Other Cost Bearer
	Internal Costs	External Costs	
Mobile Network Operator	Test Center		Taxpayer
	Information Sharing and Analysis		
	Compliance Costs		
	Cyber Protection of Customer		5G Customer
	Loss of security sensitive Customers		
		Insurance Costs of Customer	
		Lower Productivity	Security sensitive industries
		6G of Future Network Industry EU	Trusted vendors
		Loss of Sovereignty	Society
Mobile Network Operator	Insurance Costs of MNO		
	AI for Network Protection		
	Data Flow Monitoring		
	~~(Rip and Replace)~~		

All of these costs – with exemption of insurance costs of customers, loss of productivity, 6G or future network industry EU, and loss of sovereignty – , are at the same time **lifecycle costs**, meaning they will occur after the buildning of 5G networks or **external cost**, meaning costs borne by someone other than the MNO. These two characteristics constitute the smoke screen behind which these **hidden costs** are hard to see.

8.1 Test centres

Trusted 5G networks are vulnerable to attacks and subversion. Prudent governments will always wish to certify telecommunications infrastructure and supply chains independently to mitigate vulnerabilities, and because the networks and the technology is now so complex, the certification task is increasingly beyond the capacity of MNOs. Untrusted vendors raise the cost of these activities substantially, since the testing will have to be done without the vendor's cooperation, requiring broader and more thorough scrutiny, and the development of a testbed and digital 'twin' networks to understand when the real network could be being abused.

In Italy, the legislation requires (see Section 3), of all private and public operators included within the 'National Cybersecurity Perimeter', the testing of processes, technologies and software in a National Evaluation and Certification Centre (Centro di Valutazione e Certificazione Nazionale – CVCN- L. 105/2019 and 133/2019). However, a detailed analysis of impacts and costs is not yet publicly available.

An approximate approach is to take the costs for similar applied research labs as a benchmark for each respective country. Distribution of costs will depend on the degree of match-funding between government and MNOs.

As reported in the BIGS Policy paper, [1] based on estimates of the size of the market and the scale of untrusted vendors' role in each market, we estimate Italy's National Test Centre could cost **EUR 40 million** per year. The value has been calculated starting from France's estimation, proportionally considering the differences of MNO and overall mobile market sizes.

8.2 Regulatory costs.

The Italian legislation foresees the creation of a national test centre (see Section 3 and 8.1). The CVCN is part of the new national legislation of the National Cybersecurity Perimeter. However, the publication of the actuating decrees is still under discussion by the government. Nonetheless, on August 3rd 2020, it published the public call for the selection of 70 experts in computer security that will constitute the initial round of CVCN resources. [21] The private entities' costs are mainly associated to the presentation of the requested documentation and the implementation of remediations afterward. The costs for MNOs to apply the CVCN are considered the main voice of costs of regulation in Italy.

According to the cited law, the analysis of the risks associated with the object of the supply needs to be specified to the field of use, and must indicate:

- the components with which the object of the supply interacts.
- the configurations of these components.
- any existing safety measures, whether physical, technical, procedural, or related to personnel, with an indication of any certification or checks carried out.
- safety requirements that characterise the use of the object

The CVCN should complete the process in a maximum of 105 days: 45 days for the preliminary documentations (there is a speedup ticket, usable only once, that shortens this phase to 15 days, for special situations) and 60 days to complete the technical tests. After this timeframe, should no answer / impediment be reported, the activity can be initiated, based on the so-called silent-consent (in Italian "silenzio-assenso").

The working hypothesis is that the overall costs of this configuration are less than the expenses that an MNO would sustain anyway to comply with the Golden Power regulation, because the government will uphold the costs of the CVCN. Moreover, the new legislation has mechanisms to limit delays on provisioning or conclusion of a deal to a maximum value of 105 days. It is essential to underline that these costs are mandatory for the private subjects that fall under the NCP who buy HW/IT devices and services from EU and extra-EU suppliers. All the Italian MNOs fall under this category.

In the Italian case, the validation costs (though not entirely for the testing ones) are always covered by the government and the application costs are due for both trusted and untrusted vendors. In the case of untrusted vendors, the validation might take longer than usual. Since the CVCN is not yet active, there are no data on its averaged performances, but we believe a realistic hypothesis is that the **validation would be 50% longer than usual for untrusted devices**, because of the general need to perform tests that are more scrupulous.

8.3 Cost of data breaches

The BIGS Policy paper [1] introduced a calculation model to estimate the relative costs of data breaches across a 5G network, in the case of unsecure or untrusted devices. The paper also presented a formula that estimates these values, starting from the data available today and the estimated 5G network penetration, across years. What follows is the details for Italy and how the single elements of the costs model have been calculated.

8.3.1 Cybercrime trends for Italy

The report of Polytechnic of Milano [36] reports that, over the past 9 and half years, it has analysed and classified on average 99 severe attacks per month (129 in 2018, 137 in 2019 and 142 in 1H20), [36] out of a total of 10.938 severe attacks analysed from January 2011 to June 2020, 8.134 of which were from 2014.

In details:

- 873 in 2014.
- 1012 in 2015 (+14%).
- 1050 in 2016 (+3.75%).
- 1127 in 2017 (+7.4%).
- 1552 in 2018 (+37.7%).
- 1670 in 2019 (+7.6%).
- 850 in the first semester of 2020.

In 2019, the growth compared to 2018 was 7.6%, compared to 2014, which was 91.2%. The average trend of growth year on year from 2014 to 2019 is 14.1% (see the graph below). We can then assume that, for Italy, the annual growth trend is almost linear, with a gradient of about 14-15%.

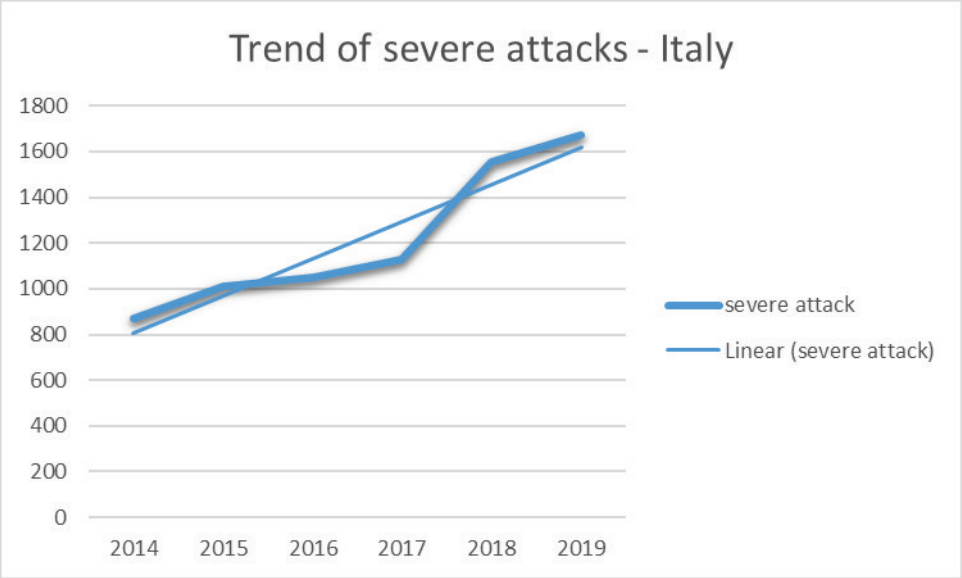

Figure 1: Trend of year-over-year attacks – Italy.

Another resource, the Annual Cybercrime Report, [37] confirms that cybercrime is expected to have an approximate worldwide growth rate of 15% per year until 2025, even following the introduction of 5G (see Table 3).

To calculate the unique impact of 5G on the data breaches, it is important to consider only the portion of a data breach that may statistically be caused by a security problem on a 5G network. A 5G network affects only data in transit. The three phases of the data life cycle are [38]: ingestion (acquisition from local sensors), data in transit, and data at rest (stored somewhere, for example in a database). A data breach could happen at any of these phases,

however, a networking problem affects only the "data in transit". Protection of the "in transit" data is critical, as data is considered less secure while in motion.

Considering the approximate growth rate of 15% per year until 2025, we can estimate a rough percentage increase of 5% for the phase "data in transit" (working hypothesis, obtained by splitting linearly the growth percentages among the various stages of the life cycle – see Table 3).

Table 3: Increase of cybercrime global.

	2021	2022	2023	2024
Annual increase of cybercrime global [37]	15%	15%	15%	15%
Annual increase of cybercrime global for the "data in transit" fraction	5%	5%	5%	5%

8.3.2 Costs of a single data breach in Italy

The IBM's report [39] indicates that the average time it took an Italian company in 2019 to identify and contain a breach was 283 days, with an average cost of USD 3.52 million, while in 2020, the value is 268 days with an average cost of USD 3.19 million.[7] The number of reported breaches for 2019 was 1276, while for 2020 the estimated value is 850 for 1H20 [36] [40].[8] For Table 4, we considered an estimated multiplication factor equal to two, based on the past years' growth rates, to calculate the value of the expected number of data breaches for the entire year, starting from the value of 1H20 and considering the average acceleration of cybercrime, following the beginning of COVID-19 pandemic. The result is a forecast of **1700** data breaches for 2020.

Table 4: Costs of a single data breach for Italy (different sources).

Average Italy results	2019	2020
Total cost of a breach [39]	$ 3.52M	$ 3.19M
Number of data breaches [40]	1276	**1700**
Time to identify and contain	283 days	268 days
Security automation deployed	49% of orgs	56% of orgs

For each year, you can assume that:

$$cost\ of\ a\ breach\ (per\ year) = cost\ of\ a\ breach\ previous\ year + annual\ increase\ of\ cybercrime\ global\ for\ the\ "data\ in\ transit"\ fraction$$

In the formula, the $annual\ increase\ of\ cybercrime\ global\ for\ the\ "data\ in\ transit"\ fraction$ is equal to 5%. The results presented in Table 5, therefore, reports the estimated costs of a breach in the period ranging from 2021 to 2024 and the estimated number of corresponding data

[7] IBM's estimation of costs includes the complete costs chain (e.g. recovery, mitigation, legal and downtime)

[8] The used sources report the number of data breaches reported because of GDPR. This only includes a fraction of the total number of data breaches because the GDPR obliges to report only those data breaches that include sensitive privacy-related data. Therefore, that the real number of data breaches might be higher should a data breach include other types of data.

breaches. The values are calculated assuming a linear yearly growth of 5% (for the "data in transit" fraction, see Table 3).

Table 5: Estimated annual Increase of data breaches only considering the "data in transit" fraction.

	2021	2022	2023	2024
Total cost of a breach	$ 3.35M	$ 3.52M	$ 3.69M	$ 3.88M
Number of data breaches	1785	1874	1968	2066

8.3.3 Dependency of the MNOs on untrusted vendors

The last step consists of the calculation of the fraction of a data breach that can be ascribed to security problems with data in transit over untrusted portions of the 5G network.

The "data in transit" can be violated over any type of network; therefore, our estimation model considers the penetration rate of the 5G networking to proportionally calculate only the portion of data that is violated due to 5G security problems.

For this calculation, we use the estimated penetration of 5G with respect to global traffic and the percentage of untrusted devices present in the MNOs networks. The working assumption is that data breaches of the 5G network are mainly a consequence of untrusted equipment. Generally, data breaches on other portions of the network are possible, but the development of 5G networks follows high standards and security-by-design criteria. From the threat modelling point of view, the differentiating aspect is the untrusted components in the system.

In 2022 and 2023, the penetration of 5G (the percentage share of 5G over the total amount of mobile connections) in Western Europe will reach an average of 26% [41] and by end-2024 will reach an average of 29%. [42] The calculation starts from 2022 because Italy expects to start the rollout of the 5G standalone (SA) that year (see Table 6).

Table 6: Estimated penetration of 5G traffic with respect to the global MNO traffic

	2022 [41]	2023 [41]	2024 [42]
Estimation of penetration for 5G vs global traffic for Western Europe	26%	26%	29%

The market share of Italian MNOs is reported in Table 7.

Table 7: Market share of Italian MNOs mobile sector (source [43])

MNOs	Market share
WINDTRE	26.1%
Vodafone Italy	29.1%
TIM	29.0%
Iliad	6.6%
Other MNOs	9.2%

In Italy, the presence of extra-EU vendors for the different MNOs, according to the public sources and interviewed stakeholders, is reported in Table 8. Interviewed MNOs however

reported that the presence of extra-EU vendors is significantly lower than that for 4G and is limited to RAN (null on the more critical core network). See also Table 10.

Table 8: Presence of extra-EU vendors in the main Italian MNOs networks

MNOs	Extra-EU vendors [44] [45] [46]
WINDTRE	ZTE
Vodafone Italy	Huawei
TIM	Huawei
Iliad	No extra-EU vendors present
Other MNOs	No extra-EU vendors present

Table 9 reports the gross national distribution of mobile telecom traffic (ISTAT, 2020 [47]) and splits it across the country districts (data from interview). These values are used to calculate the weighted distribution of overall telecom traffic in the main country districts for the year 2020.

Table 9: Gross national distribution of mobile telecom traffic 2020

	Gross national distribution of mobile telecom traffic 2020 [47]	Distribution of the global telecom traffic inside the single districts (split estimation, from interviews)	**Weighted distribution of overall telecom traffic in the main country districts (values for 2020)**
North-west	60%	50%	**30%**
North-east		50%	**30%**
Centre	40%	60%	**24%**
South		40%	**16%**

The cost of a single breach, reported in Table 5, only covers the "data in transit" portion of the data lifecycle, across any type of network, not only 5G. To estimate the impact of the 5G networks only in the hypothesis of 5G SA, the values of Table 5 must be weighted with the portion of a data breach that can be ascribed to the 5G network; for this, see Table 6 (i.e. because of security problems with data in transit over 5G) and to the untrusted vendors.

8.3.4 Estimated costs of data breaches happening over untrusted devices

The current section aims to estimate the costs of data breaches happening over untrusted devices present in the 5G network.

Table 10 reports the gross estimation of the total weighted percentage of untrusted or extra-EU 5G only devices. The value is obtained as a multiplication of its first two columns.

Table 10: Gross estimation of the weighted percentage of untrusted or extra-EU 5G-only devices.

	% of untrusted 5G only devices active in the MNOs (2020) (data from interviews and press)	MNO market share in Italy [43]	Weighted percentage of untrusted 5G only devices
WIND [44]	50%	26.1%	**13.05%**
Vodafone [44]	60%	29.1%	**17.46%**
TIM [45]	25%	29.0%	**7.25%**
Iliad [44]	0%	6.6%	**0.00%**
Other MNOs [44]	0%	9.2%	**0.00%**

One special note concerns the value for TIM. As already stated in Table 8, TIM is reported to have Huawei devices in their 5G network. Reuters reports [48] that Telecom Italia has decided to retain Nokia as a supplier and reduce Huawei's share of a planned purchase of equipment for building a 5G network to a maximum of 25%. Interviewed stakeholders reported that today's TIM network does not have a substantial dependency on extra-EU vendors; however, we included in the calculation a provisional 25% value as an upper bound value.

Table 11 reports the results of the multiplication of the "weighted percentage of untrusted 5G only devices" of Table 10 with the "estimation of penetration for 5G vs global traffic for Western Europe" of Table 6.

$$\begin{aligned} &total\ weighted\ percentage\ of\ untrusted\ 5G\ only\ traffic \\ &= weighted\ percentage\ of\ untrusted\ 5G\ only\ devices \\ &* \ estimation\ of\ penetration\ for\ 5G\ vs\ global\ traffic\ for\ Western\ Europe \end{aligned}$$

Table 11: Total weighted percentage of untrusted 5G-only traffic

	Years		
	2022	2023	2024
	26% *(value from Table 6)*	*26%* *(value from Table 6)*	*29%* *(value from Table 6)*
MNOs	Weighted percentage of untrusted **5G only traffic**		
WIND	3.39%	3.39%	3.78%
Vodafone	4.54%	4.54%	5.06%
TIM	1.89%	1.89%	2.10%
Iliad	0.00%	0.00%	0.00%
Other MNOs	0.00%	0.00%	0.00%
TOT	**9.82%**	**9.82%**	**10.95%**

Finally, Table 11 must be adjusted to consider the obsolescence of the MNO devices, based on the hypothesis that newly installed terminals would only be trusted (lower bound assumption). We assumed a year over year obsolescence ratio of 10%. Table 12 reports

the year over year value of the total percentage of dependency of MNOs by 5G traffic routed through "untrusted" vendors.

Table 12: Year over year value of the total percentage of dependency of MNOs, by 5G traffic routed through "untrusted" vendors.

2022	2023	2024
9.8%	8.8%	8.9%

8.3.5 Conclusions

Table 13 reports the estimated portion of the costs for Italy of data breaches due to security problems of 5G (i.e. mainly the working hypothesis that security issues arise with untrusted devices). The values result from the multiplication of the two values of Table 5 with the value of Table 12, converted into euro (the used conversion rate USD to EUR is 0,8168, measured in December 2020).

Table 13: Estimated portion of the costs for Italy of the data breaches, due to security problems of 5G infrastructures of untrusted vendors.

Estimated portion of the costs for Italy of the data breaches, due to security problems of 5G infrastructures of untrusted vendors		
2022	2023	2024
$ 647.146M	$ 642.130M	$ 710.672M
€ 528.58M	€ 524.48M	€ 580.46M

The final value for 2024 is approximately **EUR 580 million.**

While surprisingly low, this is because data breaches occurring over untrusted 5G bearer networks are likely to form a low proportion of overall breaches in the country. Interviews with MNOs and analysis confirmed that Italian MNOs' dependence on untrusted vendors is likely to be small, providing as little as 8.9% of total capacity (see Table 11) by 2024 if the current market share is confirmed (additionally, full 5G network coverage is expected no earlier than 2024, with about 70% of mobile traffic still over 2G-4G).

The number of reported data breaches in Italy for 2019 is unrealistically low (1276) compared to Germany (25036) [40]. In the alternative, as done for France in the BIGS Policy paper, [1] we have therefore assumed, in a second calculation, that the number of data breaches, once 5G is deployed, would increase and become at least comparable to that of Germany. In that case, the costs would be in the region of **EUR 8.548 billion**. This hypothesis is justified also by using the conclusions of the SwissRe SONAR Insurance report of 2019 [23]: *"hackers can also exploit 5G speed and volume, meaning that more data can be stolen much quicker […] interruption and subversion of the 5G platform could trigger catastrophic cumulative damage. Cyber exposures are significantly increased with 5G, as attacks become faster and higher in volume"*. Evolution in 5G adoption may lead to an increased number of breaches for Italy, closing the gap between Italian and German trends. This, in our opinion, will be a consequence of both 5G adoption and the fact that both nations are

members of the unique European data strategy to make EU a role model for a society empowered by data.

8.4 Shift of demand

As anticipated in the BIGS Policy paper, [1] the inclusion of untrusted vendors in European 5G networks might lead to the pre-contract loss of **security-sensitive clients,** and possibly even their emigration. Those clients would make sure to stay clear of suppliers that, on their part or with their clients, communicate via or process data and information in insecure 5G networks. This concerns **government clients** such as the military, intelligence, and security agencies, but also federal and state ministries and downstream institutions. Certain parts of the private sector, like **critical infrastructure or civil protection providers,** would take the same precautionary measures (see also Section 5.2).

There are various definitions of critical infrastructures, and the composition of sectors differs even among EU member countries. In Italy, the following sectors [49] are usually referred to:

- energy,
- telecommunications,
- water,
- agriculture,
- health,
- transport,
- banks financial and insurance services,
- information technology.

In this document we also consider as part of the critical infrastructures the following:

- civil protection and police force,
- infrastructures used by the government.

According to publicly available sources, [50] [51] [52] [53] [35] [54] [55] [56] the contribution of the aforementioned sectors to the Italian GDP counts for an overall value of **34.6%.**

The size of the possible shift in demand of critical infrastructure providers could be calculated using the formula in Section 6.3 of the BIGS Policy paper (chapter "Shift of Demand"). [1]

In Italy, with the following parameters, the potential shift of demand of critical infrastructure industries away from MNOs operating untrusted networks is in the range of **EUR 929 million**.

Table 14: Values used to calculate KRISIS indicator for Italy.

Revenue of telecommunication services in 2020 [57]	31576m €
Share of mobile telecommunication services of total services [57]	47.41%
Share of business customers of all customers [57]	17.94%

Relative contribution of critical infrastructure industries to GDP [58]	34.6%

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 particularly to their know-how and their research in progress.

The Italian industries that use patents, trademarks, designs, industrial models, and copyrights, i.e. with a high intensity of intellectual property rights, contribute to 46.9% of the GDP. [58] In Italy, the IPR shift of demand is in the range of **EUR 1.259 billion (**using the formula reported by [1] Section 6.3).

As reported by [1], Section 6.3, evaluating the potential shift of demand triggered by IPR-intensive industries is difficult. We are aware that there is an overlap between the IP-intensive and the critical infrastructure industry. However, some parts of KRITIS cannot necessarily be considered IPR-intensive (like water supply, agriculture, etc.), and vice versa. It is therefore safe to say that more than half, and up to two thirds, of all MNOs' sales with corporate customers are in question here and should tend to migrate towards trusted networks.

For this reason, to calculate the global shift of demand in the absence of more precise data for Italy, we estimated a total of 50% of combined contribution (by KRITIS and IPR) to GDP in 2020, proportionally comparing with the values of the other countries (Germany, France, and Portugal).

We estimate the loss of security-sensitive clients, the shift of commercial demand, for **Italy,** as more than half or **EUR 1.342** billion of revenue, with commercial customers in the telecommunications market potentially at risk of shifting towards trusted networks. Italy's 2020 market (**EUR 31.576 billion**) was less than half the size of Germany's, with only a slightly greater proportion of revenue generated through mobile telecommunications services (47.41% compared to 43.97%), and the lowest proportion of business users (18%) as a percentage of total revenues.

8.5 Redundant infrastructures

The government has one further option open to MNOs to ensure the security of the network upon which they rely: to build its own and **create a secure, redundant network if it cannot trust MNOs using untrusted vendors' equipment (**see also the wholesale model in Section 4.1).

The number of nodes, security requirements, functions needed to perform, and the overhead for a state communications provider, or at least sub-contracted MNOs, needed to operate it, make this option extremely expensive. We can estimate costs using 'top down' methods, looking at existing projects and analogous initiatives from the recent past.

As discussed in Section 5.2, Italy is one of the European countries with the most developed civil protection and emergency infrastructure. The country has several risks (maritime, territory, etc.), hence, there is a relevant number of redundant emergency networks operating (UHF/VHF, radio, TETRA etc). According to interviews, there is no official

positioning among the bodies that deal with civil protection about which infrastructures will be substituted by 5G. No official plans have been announced yet. For Italy, we estimate a gross value of **EUR 700 million**, calculated proportionally by comparing the civil protection structures and the publicly available estimations for Germany and France (see BIGS Policy paper [1]).

8.6 Costs of rip and replace

As presented in the Section 5, in Italy, a gross estimation for a Rip & Replace extended to all the subjects regulated by the GP has already been presented by COPASIR. [18] [19] The COPASIR estimated a global impact around **EUR 600 million**, without a significant delay in the development of 5G infrastructure. The value has been proportionally calculated from estimations for Australia and U.S. who already experienced a Rip & Replace of their networks.

9 Conclusions

Figure 2 summarises the hidden costs in the Italian context. The cost of data breaches, if we do not remove the extra EU manufacturers, are relatively low but, in any case, consistent and comparable with the costs of redundant infrastructure and rip and replace.

The number of reported data breaches in Italy for 2019 is relatively low (1276) compared to Germany (25036). [40] We considered a second hypothesis, in which the number of data breaches, once 5G is deployed, is equal to that of Germany. In this second case, the costs of data breaches would be in the range of **EUR 8 billion**.

Starting from the conclusions of the SwissRe SONAR Insurance report of 2019 [23]: *"hackers can also exploit 5G speed and volume, meaning that more data can be stolen much quicker […] interruption and subversion of the 5G platform could trigger catastrophic cumulative damage. Cyber exposures are significantly increased with 5G, as attacks become faster and higher in volume"*. Evolution in 5G adoption may lead to an increased number of breaches for Italy, hooking Italian trends with Germans. This in our opinion will be a consequence of both 5G adoption but also because both nations are members of the foreseen unique European data strategy, to make EU a role model for a society empowered by data. As presented in the Policy Paper [1] the most obvious costs of untrusted vendors occur when the network is being used to sabotage an entire economy. For this "Armageddon Scenario", the effect of such an act of sabotage on the Italian gross domestic product (GDP) will probably, at any rate, be comparable to that of a few days of general strike or a full lock-down during a pandemic. Based upon recent calculations conducted by the Bank Italia [34] to evaluate the effects of a nation-wide lockdown due to COVID-19 pandemic, each lost working week corresponds to 0.5 percentage point of GDP. Taking the Italian 2019 GDP of EUR 2450 billion [35] as a basis, an interruption of working life of three days would translate into an absolute amount of about **EUR 5.25 billion**, without taking into consideration cascading and other second-round effects (e.g. the costs of a then unavoidable and precipitous post-incident reactive rip-and-replace).

Cybersecurity risks of extra-EU vendors for 5G network and equipment are real and not many mitigations exist (the risk R5, reported in the NIS EU document on Risk Estimation

of the EU Toolbox, is that with less remediations). MNOs have already taken steps to reduce dependency and impact on their infrastructures (in Italy, mainly for the 5G core network) of the extra-EU devices, also looking ahead to the new NCP legislation.

Operating under the hypothesis of the Clean5G Policy paper [1], the Italian country study sought to estimate the national impact of the different costs categories. The takeaway point here is not an absolute figure, but the graphic clarification that the costs in rollout of 5G networks differ in sizes and nature.

Overall, we show in this country study that the total societal costs, i.e. including externalities, are higher over time than the potential savings that arise for mobile network operators when they use non-trusted network technology to deploy 5G. Ultimately, this evidence should convince decision-makers to give priority to the realisation of trustworthy 5G networks.

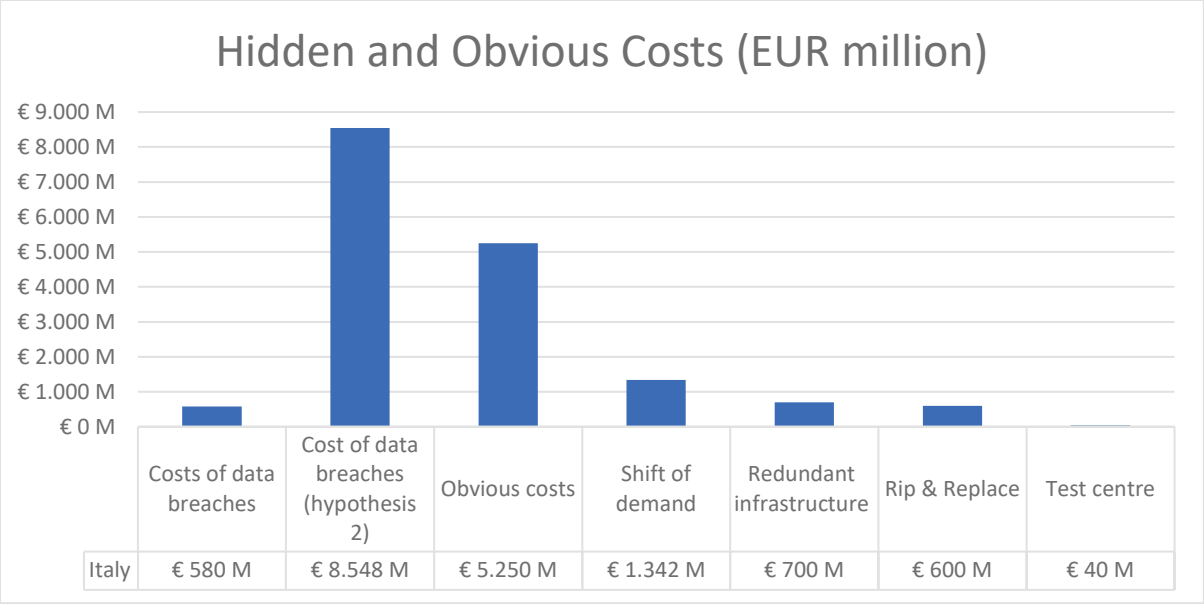

Figure 2: Range of exemplary quantifications of hidden costs (Italy, non-exclusive) (source: own calculations)

10 About the Authors

Valentina Ferrarese is a Senior Solutions Architect in the Smart Factory team at Cefriel, ICT Center of Excellence for Research, Innovation, Education, and industrial Labs partnerships. She received a degree in Telecommunications Engineering from Polytechnic of Milan. She teaches in ICT master courses and company employee's training on mobile and wireless networks. Her competences span from planning, design to testing and validation of mobile networks to Industry 4.0 end-to-end solution ideation, design, and validation at the customer plant.

Dr Enrico Frumento is a Senior Domain Specialist in the cybersecurity team at Cefriel, ICT Center of Excellence for Research, Innovation, Education, and industrial Labs partnerships. He is the author of subject-related publications and books and a member of

the European CyberSecurity Organisation. His 20+ years of research activity focuses on unconventional security, cybercrime intelligence technologies tactics and techniques, the contrast to the modern social engineering and dynamic assessment of organisations' vulnerabilities corresponding to tangible and intangible assets at risk.

Gianmarco Panza is a Senior Domain Specialist in the different networking fields at Cefriel, ICT Center of Excellence for Research, Innovation, Education, and industrial Labs partnerships. He received a degree in Information Science Engineering at the University of Padova and a master's degree in ICT at Cefriel. He teaches in ICT master courses and company employees training on next-generation networks. He has several IEEE publications in the Digital Signal Processing and Networking areas and is a senior IEEE Member. His competencies span from planning and design to testing and validation and covering the novel services enabled by the next generation of networks, as 5G and beyond.

12 Sources

[1] T. Stuchtey, C. Dörr, E. Frumento, C. Oliveira, G. Panza, S. Rausch, J. Rieckmann and R. Yaich, "The Hidden Cost of Untrusted Vendors in 5G Networks," Brandenburg Institut for Society and Security, Postdam, 2020.

[2] COPASIR, "Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale," Parlamento Italiano, 2019.

[3] Arthur D. Little, "The Race to 5G," Arthur D. Little, Luxembourg, 2019.

[4] NIS Cooperation Group, "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures," CG Publication, 2020.

[5] NIS, "Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity," NIS, July 2020.

[6] G. Carrer, "Così Huawei Italia sbuffa sul 5G," 12 11 2020. [Online]. Available: https://formiche.net/2020/11/i-com-5g-huawei/.

[7] I-COM, "Tavolo Osservatorio Sulla Sicurezza Del 5g," I-COM, november 2020.

[8] CorCom press, "5G, il Mise al lavoro sulla certificazione "cyber," 13 01 2021. [Online]. Available: https://www.corrierecomunicazioni.it/telco/5g/5g-il-mise-al-lavoro-sulla-certificazione-cyber/.

[9] CorCom press, "Sicurezza 5G, la UE agli Stati membri: completare attuazione piani entro giugno 2021," 16 12 2020. [Online]. Available: https://www.corrierecomunicazioni.it/cyber-security/sicurezza-5g-la-ue-agli-stati-membri-completare-attuazione-piani-entro-giugno-2021/.

[10] XVIII LEGISLATURA, "Indagine conoscitiva sulle nuove tecnologie nelle telecomunicazioni, con particolare riguardo alla transizione verso il 5G e alla gestione dei big data," Camera dei Deputati, Roma, 2020.

[11] Fierce, "Vodafone Ireland deploys open RAN tech at 30 sites," 19 11 2020. [Online]. Available: https://www.fiercewireless.com/tech/vodafone-ireland-deploys-open-ran-tech-at-30-sites.

[12] ComputerWeekly, "Maturing O-RAN set to have 75% market share by 2030," 22 10 2020. [Online]. Available: https://www.computerweekly.com/news/252490884/Maturing-O-RAN-set-to-have-75-market-share-by-2030.

[13] ABI Research, "Private network revenues will reach $64 bn by 2030," 25 11 2020. [Online]. Available: https://www.abiresearch.com/press/private-network-deployments-will-generate-revenues-excess-us64-billion-2030/.

[14] European 5G Observatory, "5G private licences spectrum in Europe," 23 4 2020. [Online]. Available: https://5gobservatory.eu/5g-private-licences-spectrum-in-europe/.

[15] Key4biz, “5G, da BMW a Bosch e Lufthansa. In Germania corsa alle frequenze per le reti private,” 7 4 2020. [Online]. Available: https://www.key4biz.it/5g-da-bmw-a-bosch-e-lufthansa-in-germania-corsa-alle-frequenze-per-le-reti-private/299211/.

[16] Wall Street Journal, “German Industrial Firms Plan to Build Private 5G Networks,” 6 4 2020. [Online]. Available: https://www.wsj.com/articles/german-industrial-firms-plan-to-build-private-5g-networks-11586191739.

[17] CNIT, “The 5G Italy Book 2019: a Multipespective View of 5G,” 5 12 2019. [Online]. Available: https://www.5gitaly.eu/2019/wp-content/uploads/2019/12/libro5G_2019_online.pdf.

[18] F. Bechis, “Via la Cina dal 5G. Il verdetto del Copasir,” 19 12 2019. [Online]. Available: https://formiche.net/2019/12/via-cina-5g-verdetto-copasir/.

[19] Istituto Affari Internazionali, “Europe's Manoeuvring on 5G Technology: The Case of Italy,” 24 09 2020. [Online]. Available: https://www.iai.it/en/pubblicazioni/europes-manoeuvring-5g-technology-case-italy.

[20] F. Bechis, “Huawei e 5G, ecco come (e perché) Volpi richiama Conte in Copasir,” [Online]. Available: https://formiche.net/?p=1272495. [Accessed 03].

[21] I-COM, “Il 5G per rilanciare l'Italia in sicurezza,” I-COM, 2020.

[22] Start Magazine, “Dpcm su 5G e Tim, ecco il testo,” 21 08 2020. [Online]. Available: https://www.startmag.it/?p=117301; Italian Senate, Atto n. 564, http://www.senato.it/leg/18/BGT/Schede/docnonleg/40910.htm..

[23] SwissRE, “SONAR Report: New emerging risk insights,” 5 2019. [Online]. Available: https://www.swissre.com/institute/research/sonar/sonar2019.html.

[24] United States Court of Appeals, Ninth Circuit, “UNIVERSAL CABLE PRODUCTIONS, LLC; NORTHERN ENTERTAINMENT PRODUCTIONS, LLC, Plaintiffs-Appellants, v ATLANTIC SPECIALTY INSURANCE COMPANY, Defendant-Appellee,” 04 03 2019. [Online]. Available: https://scholar.google.com/scholar_case?case=4115741785114936239&q=UNIVERSAL+CABLE+PRODUCTIONS,+LLC+v.+ATLANTIC+SPECIALTY+INSURANCE+COMPANY&hl=en&as_sdt=20006.

[25] Protezione Civile, “Strutture operative,” [Online]. Available: http://www.protezionecivile.gov.it/servizio-nazionale/strutture-operative.

[26] Italian Red Cross, “A "Jump 2019" la presentazione dell'ambulanza connessa in 5G,” 25 11 2019. [Online]. Available: https://www.crimilano.it/archivio-news/1750-a-jump-2019-la-presentazione-dell-ambulanza-connessa-in-5g.html.

[27] Oxford Economics, “Restrcting Competition in 5G Network Equipment Throughout Europe,” Oxford Economics, 2020.

[28] AGCOM, “Communication market monitoring system. COVID-19 monitoring,” 06 2020. [Online]. Available: https://www.agcom.it/osservatorio-sulle-comunicazioni.

[29] Anitec-Assinform, “Il mercato digitale in Italia 2020-2022: quale l’impatto del Covid-19,” 18 11 2020. [Online]. Available: https://www.anitec-assinform.it/news/conferenza-stampa-il-mercato-digitale-in-italia-2020-2022-quale-l-impatto-del-covid-19-.kl.

[30] Ericsson ConsumerLab, “Harnessing the 5G Consumer Potential,” 11 2020. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/consumerlab/reports/harnessing-the-5g-consumer-potential.

[31] Strand Consult, “Europe's China telecoms gear ban would cost industry $3.5 billion,” 11 2020. [Online].

[32] Analysys Mason, “5G action plan for Europe,” 11 2020. [Online].

[33] European Union, “Digital Economy and Society Index (DESI) 2020,” 09 2020. [Online]. Available: https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi.

[34] Repubblica, “Bankitalia, ogni settimana di lockdown costa all'Italia 9 miliardi di Pil. A rischio 400 mila contratti,” 1 04 2020. [Online]. Available: https://www.repubblica.it/economia/2020/04/17/news/bankitalia_bollettino_coronavirus-254283141/.

[35] Statista, “Italy: Distribution of gross domestic product (GDP) across economic sectors from 2009 to 2019,” Statista, 11 2020. [Online]. Available: https://www.statista.com/statistics/270481/distribution-of-gross-domestic-product-gdp-across-economic-sectors-in-italy/.

[36] “Security readiness: metodologie per valutare il livello di preparazione alle minacce,” Osservatorio CyberSecurity and Data Protection del Politecnico di Milano, Milano, 2020.

[37] S. Morgan, “2020 Official Annual Cybercrime Report,” 2020. [Online]. Available: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/.

[38] N. Lord, “Definition of Data In Transit vs. Data At Rest,” 15 07 2019. [Online]. Available: https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest.

[39] IBM, “Cost of a Data Breach Report,” November 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/.

[40] DLA Piper, “DLA Piper GDPR Data Breach Survey 2020,” 20 01 2020. [Online]. Available: https://www.dlapiper.com/it/italy/insights/publications/2020/01/gdpr-data-breach-survey-2020/.

[41] E. Qi, “5G Mobile Connections Will Cross the Milestone of 1.7 Billion in 2023,” 23 07 2020. [Online]. Available: https://www.counterpointresearch.com/5g-mobile-connections/.

[42] C. Donkin, “5G connections to hit 1.5B by end-2024 – Ericsson,” 27 11 2018. [Online]. Available: https://www.mobileworldlive.com/featured-content/home-banner/5g-connections-to-hit-1-5b-by-end-2024-ericsson.

[43] AGCOM, “Communication Markets Monitoring System,” 4 2020. [Online]. Available: https://www.agcom.it/osservatorio-sulle-comunicazioni.

[44] Corriere delle Comunicazioni, “Tim, la gara 5G alle battute finali: un vendor fuori dai giochi?,” 30 01 2020. [Online]. Available: https://www.corrierecomunicazioni.it/telco/5g/tim-la-gara-5g-alle-battute-finali-un-vendor-fuori-dai-giochi/.

[45] HD Blog, “TIM: nessun problema nello sviluppo del 5G senza Huawei,” 07 09 2020. [Online]. Available: https://www.hdblog.it/huawei/articoli/n526096/tim-huawei-problema-sviluppo-5g/.

[46] Le Formiche, “5G e non solo. Ecco come (e perché) l’Italia mette al bando la Cina. La vera storia!,” 22 08 2020. [Online]. Available: https://formiche.net/2020/08/5g-non-solo-perche-litalia-mette-al-bando-la-cina-la-vera-storia/.

[47] Istituto Nazionale Statistiche (ISTAT), “Rapporto sul Territorio 2020. Ambiente Economia e Società,” 2020. [Online]. Available: https://doi.org/10.1481/Istat.RapportoTerritorio.2020.

[48] Reuters, “Telecom Italia to retain Nokia as supplier, curbing Huawei's share of 5G radio network - sources,” 23 12 2020. [Online]. Available: https://news.yahoo.com/telecom-italia-retain-nokia-supplier-115326317.html.

[49] Wikipedia, “Critical Infrastructure,” 6 1 2020. [Online]. Available: https://en.wikipedia.org/wiki/Critical_infrastructure.

[50] V. Assolombarda, Interviewee, *Il settore energetico vale 11 miliardi di euro*. [Interview]. 14 November 2019.

[51] Webuild Group, “Investire nelle infrastrutture,” 4 8 2020. [Online]. Available: https://www.webuildgroup.com/it/storie/investire-nelle-infrastrutture.

[52] First Online, “Quanto vale l’acqua? Quasi 1/5 del Pil,” 14 10 2020. [Online]. Available: http://www.firstonline.info/quanto-vale-lacqua-quasi-1-5-del-pil/.

[53] Nordea, “The economic context of Italy,” Nordea, 1 2021. [Online]. Available: https://www.nordeatrade.com/en/explore-new-market/italy/economical-context.

[54] EU Commission, “State of Health in the EU - Italia - Profilo della Sanità 2019,” 2020.

[55] Assimform, “Il settore IT guida la trasformazione digitale del paese,” Assinform, 4 12 2017. [Online]. Available: https://www.assinform.it/sala_stampa/dati-di-mercato-ict/anitecassinform/il-settore-it-guida-la-trasformazione-digitale-del-paese.kl.

[56] Il Manifesto, “Forze di polizia, in Italia abbondano. Spese e personale sopra la media europea,” 08 12 2019. [Online]. Available: https://ilmanifesto.it/forze-di-polizia-in-italia-abbondano-spese-e-personale-sopra-la-media-europea/.

[57] AGCOM, “Relazione annuale 2019 - capitolo 3 - Il contesto economico e concorrenziale: assetti e prospettive dei mercati regolati tabella 3.1,” 2019.

[58] ANSA, “In Italia 7 milioni di posti lavoro da proprietà intellettuale,” ANSA, 11 12 2020. [Online]. Available: https://www.ansa.it/europa/notizie/proprieta_intellettuale/approfondimenti/2019/12/11

/in-italia-7-milioni-di-posti-lavoro-da-proprieta-intellettuale_df16c5c7-ce77-4680-8b64-9950eaac0b9b.html.

[59] Y. Golan, "Why insurers, reinsurers should care about silent risk exposures," 03 06 2018. [Online]. Available: https://www.propertycasualty360.com/2018/07/03/why-insurers-reinsurers-should-care-about-silent-risk-exposures/?slreturn=20201027113433.

[60] Statista, "Market share of mobile network providers in Italy in 2019," [Online]. Available: https://www.statista.com/statistics/548650/market-share-of-mobile-operator-revenue-in-italy/.

[61] K. Aaron and R. A. Scott, "A federal backstop for insuring against cyberattacks?," 27 09 2019. [Online]. Available: https://www.brookings.edu/blog/techtank/2019/09/27/a-federal-backstop-for-insuring-against-cyberattacks/.