BIGS

BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

# THE HIDDEN COST OF UNTRUSTED VENDORS IN 5G NETWORKS

## STATE OF DISCUSSIONS AND ESTIMATIONS

## PORTUGAL

Carlos Oliveira

---

Brandenburg Institute for Society and Security gGmbH

December 2020

## Contact and further information:

Carlos E.F. Oliveira

E-mail: carlos@nomadriver.co

Brandenburg Institute for Society and Security gGmbH (BIGS)
Executive 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

# Executive Summary

In an unregulated market, non-trusted vendors might have an advantage when mobile network operators (MNOs) focus primarily on a pricing strategy that is geared towards short to medium-term gains.

Even though Portugal's regulatory framework for 5G is expected to evolve quite dramatically during 2021, as of today there are no significant restrictions imposed on Communication Service Providers (CSPs) regarding adoption of potentially untrusted vendors for their networks (core infrastructure or radio access). The democratisation of the field of play, with new entrants coming onto the scene and deploying their own equipment, could also potentially impact the situation even if no regulatory intervention is performed.

Despite the comparatively small size of the Portuguese economy, relative to its European counterparts, a large portion of GDP is at stake from interventions, and the scale of both obvious and hidden costs would pose significant challenges to the Portuguese economic fabric.

The costs of removing untrusted vendors from Portuguese networks, as proposed by past studies, are not as significant as the abovementioned costs, according to both our own and other research, and are relatively small when compared to our realistic and Armageddon impact scenarios for compromised infrastructure.

Portuguese stakeholders run a moderate to high risk in a dynamic environment of incurring hidden costs from untrusted 5G vendors.

## Introduction & State of Debate (as of Oct 31, 2020)

The introduction of 5G in Portugal, much like in the rest of the world, has been mired with high expectations for its transformational impact on the innovation and economic landscapes in the country. However, the development has not been without its fair share of controversy and public debate.

There were high ambitions at the beginning of the process. The national regulator promoted a record amount of spectrum available for auction, and opened the national market to new entrants. This liberalised many of the competitive aspects of the Portuguese telecommunications sector, thus creating the conditions for 5G to flourish, with new public and private networks and operators emerging. However, this has since created a legislative and legal battleground between the national regulator and incumbent CSPs,, who believe they are being unfairly treated and demand equal footing in the new competitive landscape.

These challenges come side by side with the EU-wide introduction of the EU Toolbox of Risk Mitigating Measures, which Portugal has considered as a key driver for its plans (yet to be made publicly available) for 5G deployment and cybersecurity countermeasures. This is in light of the well-known and well-recognised threat vectors associated with massification of access and end-user devices, complex vendor and supplier landscapes with geopolitical implications, and the interconnected and unpredictable nature of software-based networks and new radio access network configurations.

The Portuguese government has stated that it will legislate in full alignment with EU-wide measures,[1] and that it will put in place regulation to certify and authenticate providers in the national 5G landscape. These commitments have yet to materialise, despite the auction being very much underway as of today. The following report looks at the current state of debate, the obvious and hidden costs of introducing potentially untrusted vendors, and the impact of their participation in the network.

In 2011, the 4G auction in Portugal saw Telco Operators invest EUR 372M in 4G LTE technology.[2] These operators were TMN (now Altice MEO), Optimus (now NOS) and Vodafone. This fell below the Portuguese state's expectation of selling all of the auctioned spectrum at a total budget of €429M. The table below shows the latest allocation to each operator.

| **Operator** | ***Downlink*** | | ***Uplink*** | | **Bandwidth (MHz)** | **Technology** |
|---|---|---|---|---|---|---|
| MEO | 791,000 | 801,000 | 832,000 | 842,000 | 800 | Tech Neutral |
| MEO | 950,900 | 958,900 | 905,900 | 913,900 | 900 | LTE |
| MEO | 1845,000 | 1865,000 | 1750,000 | 1770,000 | 1800 | LTE |
| MEO | 2149,900 | 2169,700 | 1959,900 | 1979,700 | 2100 | UMTS |
| MEO | 2670,000 | 2690,000 | 2550,000 | 2570,000 | 2600 | Tech Neutral |
| NOS | 811,000 | 821,000 | 852,000 | 862,000 | 800 | Tech Neutral |
| NOS | 943,100 | 950,900 | 898,100 | 905,900 | 900 | LTE |
| NOS | 1825,000 | 1845,000 | 1730,000 | 1750,000 | 1800 | LTE |

[1] https://www.anacom.pt/render.jsp?contentId=1507487

[2] https://www.dinheirovivo.pt/especial/vodafone-business-conference/anacom-massificacao-e-custos-de-equipamentos-serao-determinantes-no-5g-12778288.html

| | | | | | | |
|---|---|---|---|---|---|---|
| NOS | 2130,100 | 2144,900 | 1940,100 | 1954,900 | 2100 | UMTS |
| NOS | 2650,000 | 2670,000 | 2530,000 | 2550,000 | 2600 | Tech Neutral |
| Vodafone | 801,000 | 811,000 | 842,000 | 852,000 | 800 | Tech Neutral |
| Vodafone | 930,000 | 935,000 | 885,000 | 890,000 | 900 | LTE |
| Vodafone | 935,100 | 943,100 | 890,100 | 898,100 | 900 | LTE |
| Vodafone | 1805,000 | 1825,000 | 1710,000 | 1730,000 | 1800 | LTE |
| Vodafone | 2110,300 | 2130,100 | 1920,300 | 1940,100 | 2100 | UMTS |
| Vodafone | 2570,000 | 2595,000 | | | 2600 | Tech Neutral |
| Vodafone | 2630,000 | 2650,000 | 2510,000 | 2530,000 | 2600 | Tech Neutral |

In 2020, for the 5G auction, the government expects to be able to auction €237.9M, with 58 frequency slots available, but with many frequencies still being released from other services or still under previous licensing agreements.

There is also a fundamental difference in the auction of 2020. The original public consultation had 505 commenters, which, along with the impact of COVID-19, led to delays in the auctioning process which should, however, be concluded by the end of Q1 2021. Many of these comments pertain to opening up the process to new entrants, which can reserve spectrum and access national roaming, increasing competitiveness. Any new entrant will be subjected to covering 25% to 50% of the national population, 3-6 years after purchasing the spectrum, and to ensuring their broadband offerings support at least 30Mbps of download debit. Accompanying this, the new rules also formulate the need to ensure 5G-compatible services to hospitals, universities, industry parks, ports, airports and military institutions, be it with their own infrastructure, shared infrastructure or by resorting to an OEM offering.

Initially, the Portuguese timeline for 5G deployment was to have at least 2 cities covered by the infrastructure by the end of 2020. This would extend to all major municipalities, hospitals, universities, research institutes and other key sites by the end of 2023, and to 90% of the population by the end of 2025. Currently, the plan is for the auction to take place in December 2020 and for all procurement procedures to be finalised in Q1-2021, pushing all other dates forward, and also postponing critical decisions that need to be made around vendor procurement.

Moreover, the current auctioning procedure is still subject to litigation by the three key operators, who argue that new entrants will unduly benefit from special conditions and harm the market's competitiveness. The Portuguese regulator ANACOM, on the other hand, claims to be doing this in order to increase competitiveness and to combat the incumbents' largely established customer base.

Despite these delays in regulatory frameworks and in the 5G implementation roadmap, the three large Telco operators have already stated they will not use Huawei in the core network infrastructure. This is despite the fact that there has not been a clear ruling by the Portuguese government on whether there will be a ban on the Chinese network equipment provider, even though there has been repeated pressure from the European Commission to protect national 5G infrastructure.

Vodafone has stated they will use Ericsson equipment, a longstanding partner, while NOS (who is said to be partnering with Nokia) and Altice (who is said to be procuring a CISCO-based core network

implementation) have publicly stated they will avoid Huawei in the core.[3] Yet the MNOs have not stated what kind of protocols for their radio access networks will be applied for procuring vendors (and which vendors).

Recently, the US Under Secretary of State and the US Embassy to Portugal have stated that they would prefer if Portugal did not incorporate any Huawei equipment in its 5G network, particularly as they are both members of NATO and regularly exchange classified information. The Portuguese government, in its response, did not, however, commit to doing so beyond the particulars of any EU-wide agreements (such as the aforementioned Toolbox) and stated that when it came to systems that threatened national security or defense systems, its evaluation criteria should safeguard these requirements against ill-intentioned actors.

On the 7th of February 2020, the Portuguese government mandated the creation of a taskforce within its CSSC (*Conselho Superior de Segurança do Ciberespaço*), or High Council for Cyberspace Security, which will be responsible for assessing and assisting:

1) The implementation and operationalisation of the EU Toolbox of risk-mitigating measures.
2) To periodically revise the cybersecurity risks affecting 5G networks and help with the EU-wide assessment of said risks.
3) To produce a report that outlines the necessary actions and roadmap for cybersecurity and other measures.
    a. While this report is said to already have been made available to the government, it has not been made public, and has in fact been referred to as classified,[4] despite parliamentary pressure to release its finding. The only public recommendation is that which is behind the commentary referenced above. The Portuguese press reports that the government's current position is that the security of networks should be promoted by equipment certification and approval, and not by exclusion of vendors. This exclusion can, however, happen as a part of said certification and approval activity, as well as ongoing risk assessment activity.[5]
    b. This would align the Portuguese approach to part of the recommendations offered within the EU Toolbox, but distance it from the measures undertaken by some of its other European counterparts, who have imposed stringent bans on the Chinese manufacturers.

[3] https://expresso.pt/economia/2020-03-06-Huawei-nao-vai-integrar-o-nucleo-da-rede-5G-em-Portugal

[4] https://eco.sapo.pt/2020/09/29/governo-nao-divulga-e-classifica-relatorio-de-risco-do-5g-como-secreto/

[5] https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2020-06-05-governo-portugues-nao-vai-impedir-huawei-ou-qualquer-outra-marca-de-fornecer-tecnologias-5g/

## Alleged Costs of Market Intervention by Banning Untrusted Vendors

In its "Restricting competition in 5G network equipment throughout Europe", Oxford Economics states that over €63M would have to be spent annually (until 2023) in Portugal as a result of impeding Huawei and ZTE from competing in the market. Over €1M people would have delayed access to 5G by 2023 and over €500M would be permanently lost to the national GDP as a result of these delays. With 11,900,000 mobile phone contracts in Portugal, this would translate to an additional 5€ cost per contract. That loss of GDP, in perspective of the overall population size, would amount to circa 49€ per capita.

The assumptions underlying their baseline and post-COVID curves, however, can and should be examined. On the one hand, they examine the percentage of the population covered, and extrapolate the results of that coverage into GDP impacts. The reality of the country is substantially different, with two large metropolitan areas (Lisbon and Porto) accounting for roughly 50% of GDP and the following 8 administrative divisions accounting for roughly another 27%. Since all of these regions are anchored around key metropolitan areas, there is a direct economic incentive for Telco operators to procure technology and services to help secure the deployment of 5G technology to these populations very early on, particularly with the introduction of external competitors to the Portuguese market.

Beyond population coverage, the timelines and lead time to cover 90% of the population do not align with those of the Portuguese government upon which the procurement procedures for 5G spectrum will be based. They also do not account for the potential introduction of new players in the Portuguese telecommunications sector, which would increase competitive pressures and result in accelerated uptake and better consumer bargaining power.

Other studies have since questioned these numbers and extrapolated that many of the existing infrastructure would have to be phased out and replaced anyway. The cost incrementality is not as relevant as the Oxford Economics studies suggest. Moreover, the study disregards the direct, obvious and hidden costs of untrusted vendors, including those outlined in the EU toolbox.

**For Portugal**, with populations so heavily concentrated in few districts, rollout will rapidly reach huge swathes of the population, meaning GDP loss-projections should not be regarded as linear. Government-driven delays to 5G spectrum auction and regulation are almost certain to be the systemic issue, rather than shifts to new vendors.

# Obvious Costs of Malicious Vendors

## Estimate of Sabotage / intentional outage

In Portugal, an estimated 6.5% of GDP is lost every 30 days the economy is stopped, according to estimates by the Ministry of Finance. If there is intentional sabotage or an intentional outage caused by a malicious vendor, this is the range of costs the economy would be subjected to. The Ministry of Finance also estimates that these costs deteriorate as time progresses in a non-linear fashion, with the monthly impact naturally growing even larger with each additional day the economy is prevented from operating normally. With financial, governmental and enterprise institutions so reliant on the telecommunications infrastructure, there is non-negligible risk to relying on networks that are subject to sabotage and outages. This, of course, is incremental atop the human, environmental and other externalities.[6]

## Estimates from Shocks of Natural Causes

SIRESP, the national emergency communication system, mentioned later under the section on Redundant Infrastructure, was under great public scrutiny after it stopped working during the summer while the country was being subsumed by forest fires, with loss of land and life. While not the result of sabotage, in 2017, these fires ravaged the country and SIRESP, responsible for keeping the network operating and emergency teams in constant communication, failed repeatedly and intermittently. This created a situation in which the various emergency response services were unable to coordinate securely and in a timely manner, and had to resort to external networks and self-made protocols, with resulting costs estimated to be upwards of €613M. This speaks to the volume of external damage resulting from an inability to coordinate in emergency situations, due to network failure.[7]

## Estimates from Strike Shocks

In 2019, a strike by the union for lorry drivers of dangerous materials (including oil and gas) paralysed the country for days. Estimates by the food industry placed the damages caused by the strike at €21M per day for this primary sector, an indication of the extent to which a failure of an infrastructural sector affects the economy.[8]

# Hidden Costs of Untrusted Vendors

## Test Centres - Centres for the assessment and certification of 5G hardware, software and network operation.

Even 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. As the networks and the technology nowadays are so complex, the certification task is increasingly beyond the capacity of MNOs. Untrusted vendors theoretically 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

[6] https://www.jornaldenegocios.pt/economia/detalhe/centeno-queda-do-pib-e-de-65-por-cada-30-dias-uteis-com-economia-parada

[7] https://www.sabado.pt/portugal/detalhe/os-custos-associados-ao-incendio-de-pedrogao-grande

[8] https://www.publico.pt/2019/08/05/economia/noticia/portugal-fresh-estima-prejuizo-diario-21-milhoes-impacto-greve-1882443

testbed and digital 'twin' networks to understand when the real network could be abused. For Portugal, setting up such a test centre could cost as much as €20M. This estimate would place the Portuguese Test Centre in the cost vicinity of other reference R&D centres in the country, such as INESCTEC.

## Regulatory Costs

In Portugal, the UTAIL (Portuguese for Technical Unit for Regulatory Impact) was created to examine the costs of rules and regulations as they come from parliamentary mandates and are written into law. Since its initial inception in 2017, the unit has detected some regulatory introductions that would have an impact in the range of €20 to €30M should they pass. There is, of course, a cost to monitoring, effecting and operationalising legislative procedures that should be taken into account when considering the introduction of untrusted vendors. There will also be a cost to the legislative frameworks still to be brought to the fore as a result of complying with the EU Toolbox, especially if still granting permission for these potentially untrusted vendors to operate. [9]

One recent regulation that has been subjected to UTAIL's scrutiny is GDPR.[10] Looking at the impact that the regulation would have on businesses of all sizes, the total cost of regulation for Portugal was estimated at €126M. This entails new data protection measures, hiring human resources and implementing appropriate processes to comply with the legislation. In the case that corporations would have to adopt and strengthen their data protection measures to protect themselves against the hazard of an untrusted middleman, it is not surprising that similar costs could arise.

## Cybercrime and Data breaches

CERT, part of the National Cybersecurity Center, states that, in 2019, 62 attacks per month took place and were detected (a 29% increase YoY).[11] In 2020, this trend increased drastically as COVID hit and a much larger percentage of the population moved to remote and teleworking.

The trend is as follows:

- 248 in 2015
- 413 in 2016 (66% increase on previous year)
- 501 in 2017 (21%)
- 599 in 2018 (19%)
- 752 in 2019 (26%)
- 2075 in 2020 (176% Q1, bolstered by COVID)

Even if we exclude 2020, the average rate of growth in Portugal has been 33% per year. If we add 2020, that number almost doubles to 61%. Even if we assume that after COVID we will see a stabilisation and regression to previous (decelerated) numbers, Portugal will likely still continue to grow above the world average.

*Table 1 – Number of Incidents reported by CERT.PT*

| **Year** | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|
| **Number of incidents** | 248 | 413 | 501 | 599 | 752 |

[9] https://www.dn.pt/portugal/custa-quanto-governo-vai-medir-impacto-das-novas-leis-na-vida-dos-cidadaos-9422655.html

[10] www.jurisapp.gov.pt/media/1109/ail-rgpd.pdf

[11] https://www.cncs.gov.pt/observatorio/relatorios/

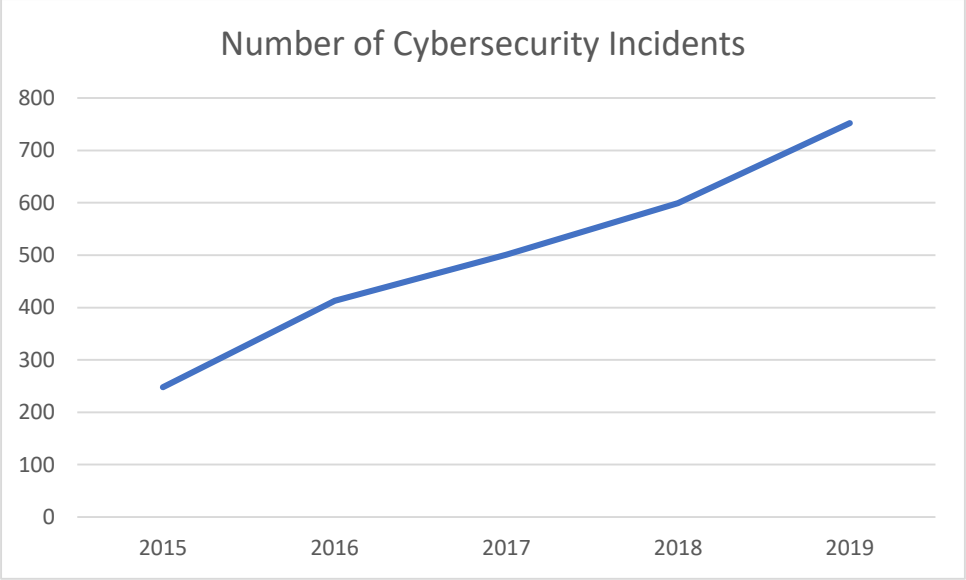



*Figure 1: Trend of attacks – Portugal*

According to the Annual Cybercrime Report,[12] cybercrime is expected to have an approximate worldwide growth rate of 15% per year until 2025, even following the introduction of 5G (see Table below). The three phases of the data life cycle are: ingestion (acquisition from local sensors), data in transit and data at rest. Nonetheless, even if a data breach could happen at any of these phases, only the "data in transit" involves 5G. Wherever data is moving, effective data protection measures for data transit are critical as data is often considered less secure while in motion.

Therefore, from the approximate world growth rate of 15% per year up to 2025, we can estimate a rough percentage increase of 5% for the phase "data in transit" (by dividing the percentages linearly between the various stages of the life cycle – see Table 1). For Portugal, we can assume these percentages are slightly higher, as the volume of attacks is growing at practically double the world average.

*Table 2: Estimated Increase of Cybercrime in Portugal*

| | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|
| Estimated annual increase of cybercrime in Portugal (Linear increase) | 33% | 33% | 33% | 33% |
| Annual increase of cybercrime global for the "data in transit" fraction | 11% | 11% | 11% | 11% |

[12] https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

## Cost of a Breach

An IBM report indicates that the average time it took an Italian company in 2019 to identify and contain a breach was 283 days. Even though no data is offered for Portugal, both countries' ICT industries represent a similar percentage of value added relative to GDP (circa 3%).[13] One may assume there is similar maturity in response and capacity. The same report estimates the cost per attack at $3.19M. Assuming the GDP ratio between both countries apply, with the Portuguese economy roughly 12% of its Italian counterpart, a similar figure for Portugal would represent 383K. In 2020, applying the same proportion would place Portugal's average cost per data breach at $424K. The number of reported breaches for 2019 was 752, while for 2020 the estimated value is 2075.

*Table 3: Portugal's results*

| Average results for Portugal | 2019 | 2020 |
|---|---|---|
| Total cost of a breach | $424k | $383k |
| Number of data breaches | 752 | 2075 |
| Time to identify and contain | 283 days | 268 days |

The following table shows the cost of a breach (calculated with the above defined formula) from 2021 to 2024 and the number of data breaches from 2021 to 2024 (calculated with the same method).

*Table 4: Increase of global cybercrime in "data in transit" fraction.*

| **Year** | **2021** | **2022** | **2023** | **2024** |
|---|---|---|---|---|
| *YoY Growth* | *33%* | *33%* | *33%* | *33%* |
| **Cost of breach** | **$0.47M** | **$0.52M** | **$0.58M** | **$0.64M** |
| **Breaches per year** | **2303** | **2557** | **2838** | **3150** |

## Fraction of a data breach over 5G

The last step is to calculate the fraction of data breaches that can be ascribed to security problems with data in transit over 5G. For this fraction, we use the penetration estimation of 5G in respect of the global traffic. In 2023, 5G penetration (the percentage share of total mobile connections) will reach an average of 26%[14] in Western Europe and an average of 29%.[15]

[13] https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_sector_-_value_added,_employment_and_R%26D#The_size_of_the_ICT_sector_as_measured_by_value_added

[14] 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/.

[15] [5] 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.

*Table 5: Estimated penetration of 5G in Western European traffic.*

| | 2022 | 2023 | 2024 |
|---|---|---|---|
| Penetration estimation of 5G vs global traffic | 26% | 26% | 29% |

The cost of a breach reported in Table 3 refers exclusively to the "data in transit" portion of traffic, whereas the total sum of data also includes data at rest and data in processing. To further estimate the impact of breaches as applied to 5G, the values of Table 3 must be weighted with the fraction of a data breach that can be ascribed to the 5G network. For this, see Table 4 (i.e. breaches specifically attributed to security problems with data in transit over 5G).

Finally, we have to estimate the portion of a data breach that happens, on average, during the "data in transit", on a 5G network controlled by an "untrusted" device. For this last step it is necessary to calculate the percentage of dependency of telco operators on untrusted vendors. As interviews show, in Italy, the dependency of the telco operators on untrusted vendors is only partial.

A recent estimation reports that the percentage of dependency of telco operators on untrusted vendors is expected to be, on average, 30% in 2022. We assume an obsolescence rate of 10%, with European vendors assuming responsibility for replacements.

*Table 6: share of dependency on untrusted traffic*

| **% of dependency on untrusted traffic for 5G only** | | |
|---|---|---|
| **2022 [7]** | **2023** | **2024** |
| *8.9 %* | *8.0%* | *8.0%* |
| | | |
| *O*bsolescence % per year | 10% | |

## Cost Scenarios

The scenario reported below describes a situation where all untrusted devices in a 5G network receive commands to commit a data breach and exfiltrate data. In this situation, the portion of a data breach that is ascribed to the untrusted portion of a 5G network can be calculated as follows:

$$pca_t^{br\ 5G\ ctry} = \left(c_{t-1}^{br\ ctry} * \frac{1}{3} * r_t^{cc\ ctry} + c_{t-1}^{br\ ctry}\right) * \sum_{mno=1}^{n} \left(dsh_t^{mno\ ud\ ctry} * msh_t^{mno\ m\ ctry}\right) * \left(pen_{t-1}^{5G\ ctry} * \left(1 - obs_t^{5G\ ctry}\right)\right) * n_t^{br\ ctry}$$

with

$pca_t^{br\ 5G\ ctry}$ = estimated portion of the aggregated costs of the data breaches, due to security problems of 5G, in respective country in time period year t

$c_{t-1}^{br\ ctry}$ = total cost of a breach, in respective country in time period year t-1 (last year)

$r_t^{cc\ ctry}$ = increase of cybercrime, in respective country in time period year t

$dsh_t^{mno\ ud\ ctry}$ = % of untrusted 5G only devices active in the MNOs, in respective country in time period year t

$msh_t^{mno\ m\ ctry}$ = MNO market share in respective country, in respective country in time period year t

$pen_{t-1}^{5G\ ctry}$ = penetration estimation of 5G vs global traffic, in respective country in time period year t-1 (last year)

$obs_t^{5G\ ctry}$ = obsolescence % of the 5G existing terminals (substitution rate, in respective country in time period year t

$n_t^{br\ ctry}$ = total number of breaches, in respective country in time period year t

$t$ = time period, year of consideration

leading us to the following results:

*Table 6: estimated portion of cost for customers of a (single) data breach, due to security problems of 5G (Realistic scenario)*

| **2022** | **2023** | **2024** |
|---|---|---|
| $0.046M | $0.046M | $0.052M |

*Table 7: total costs of data breaches per year, Portugal (Realistic scenario)*

| 2022 | 2023 | 2024 |
|---|---|---|
| €96.72M | €107.25MM | €132.65M |

## Quantification of order of magnitude of potential losses

A **second approach** to be considered is to think about the '**order of magnitude' costs of different events** (cases) against a logarithmic scale. Such a scale for the measurement of prejudices helps to better differentiate four scenarios – below – according to their severity, and to better show the very important differences between them.

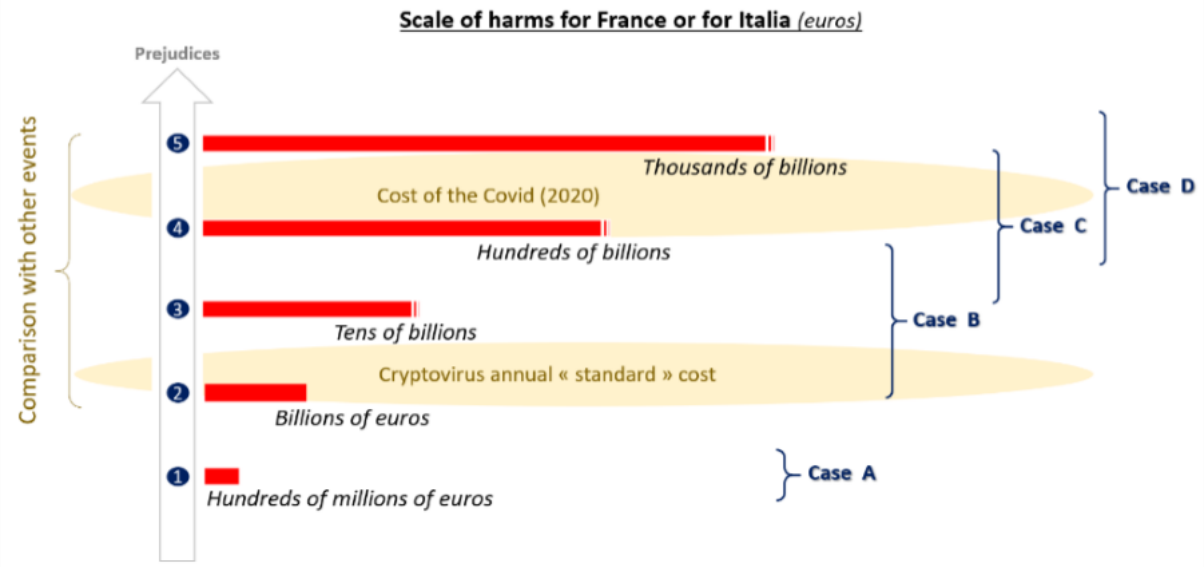
**Case A -** A complete and definitive blockade of 100% of the telecommunication infrastructures of one MNO, causing a blackout of personal and business phone calls, SMS, MMS, & mobile internet services.

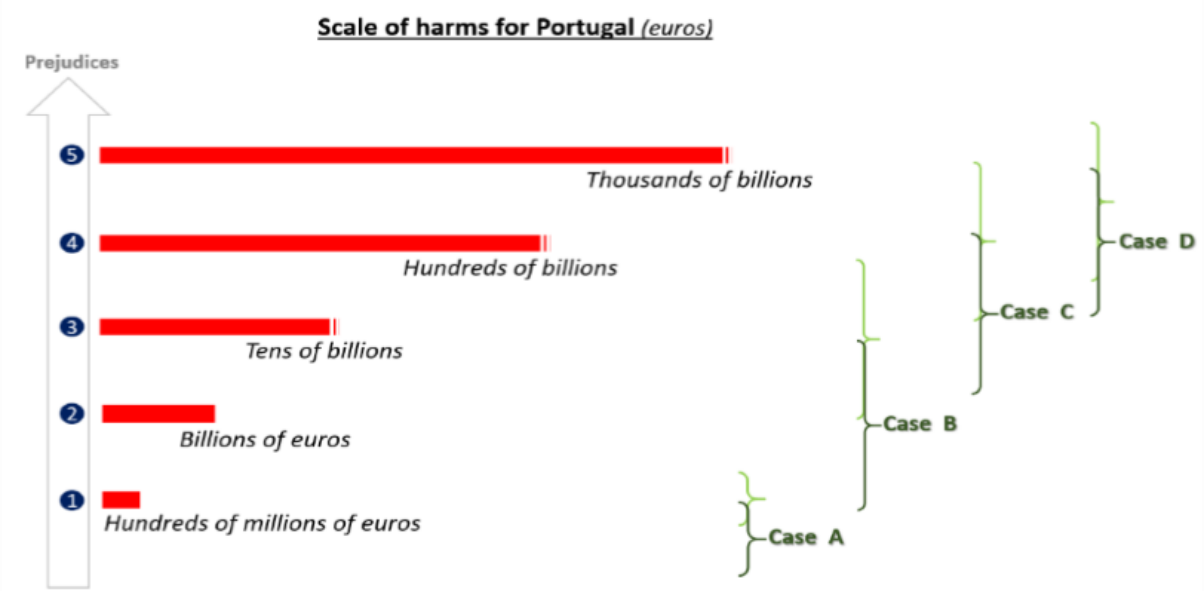
**Case B** – The blockade also affects IoT, industrial uses (Factory 4.0…), or communicating vehicles.

**Case C –** In addition to A and B, there is an attack on data, programs and software (owned by people, enterprises, associations, administrations) through the 5G infrastructure provided by one provider, resulting in their definitive destruction, encryption or inaccessibility.

**Case D** – In addition to case C there is also falsification of these data, programs and software, causing automobile, train or ship accidents, domestic accidents, and medical and industrial disasters.

As economies of similar size, **France** and **Italy** are likely to suffer similar losses against each of the cases. As the smallest economy in the Clean5G study, **Portugal** is likely to suffer the least in absolute terms, but not insignificantly relative to its size (dark green vs France in light green). For details on the premises behind this calculation, please see the country study for France as the basis for the original calculation.




## Shift of Demand

### Critical Infrastructure

The official definition of critical infrastructure in Portugal is particularly reductionist, circumscribing it to energy and transportation – a definition that the government itself has said to be under review to align it further with other EU-wide definitions.[16] Infrastructure sectors defined as constituting

[16] https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBAAAAB%2bLCAAAAAAABACzNLYwAgCF3gJVBAAAAA%3d%3d

critical infrastructures in Portugal (see illustration below) contributed, in 2017, approximately 12% of overall gross value added.[17]

| Sector | Subsector |
|---|---|
| **Energy** | Electricity |
| | Oil |
| | Gas |
| **Transportation** | Road |
| | Rail |
| | Air |
| | Inner Country Waterways |
| | Maritime |

Sectors defined as critical infrastructure, as adopted by the Portuguese government in 2011.

These sectors are not reflected in national accounting one-to-one. It is still possible to derive approximate values for at least some of them.

**Assuming** that this proportion is reflected in the structure of customers of the telecommunication sector – a quarter of the customers belonging to critical infrastructures – we derive that approximately 12% of the turnover of the communication sector (the public sector and corporate customers, not private end user customers) might shift, in the case that untrusted vendors are kept in the Portuguese 5G network. Customersfrom critical infrastructures would either switch to providers that work exclusively with trusted network equipment vendors, build their own campus networks, or even decide against using 5G technology altogether (and instead operate 4G/ WLAN technology), at least in particularly security-sensitive applications.

While the first shift – customers switching operators – is rather a business-management consideration for the operators making decisions about their choice of vendors, it nonetheless falls into the category of hidden costs. The necessity to build and operate campus networks, on the other hand, comes at an economic cost – namely, a crowding-out effect on investment and an opportunity cost. The third aspect comes with foregone productivity gains.

The turnover of the telecommunication service industry – not even looking at telecommunication infrastructure and end devices –for 2019 in Portugal is estimated to amount to €3.55 billion. Of this, mobile telecommunication services represent about 81% of all revenues,[18] as most are bundled into 2/3/4/5-play packages, by far the most common subscription method in the country. Business customers represent approximately 28% of all revenues. Therefore, the 12% mentioned above corresponds to an absolute figure of €97.23M Euro that could be shifted from current MNOs to other MNOs, rerouted into campus networks, or invested in the maintenance of obsolete but trusted and less efficient technology. The foregone productivity gains in the latter case are hard to estimate.

[17]https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_cnacionais2010b2016&perfil=392022253&INST=391941652&contexto=am

[18] https://anacom.pt/streaming/SectorComunicacoes2019.pdf?contentId=1530341&field=ATTACHED_FILE

### IPR-Intensive Industries

Using the same methodology as above, if one applies the rationale to shift of demand from IPR-intensive industries (rather than critical infrastructure), which represent about 42.5% of Portuguese GDP, costs could rise as high as €344.4M.

### Total

An aggregate estimated total would represent approximately 48% of the GDP. Adopting the same assumptions about the percentage of revenues that would shift from telco operators with unknown vendor infrastructure, this could lead to a demand shift of up to €388.9M.

## Redundant Infrastructure

SIRESP, a national emergency telecommunications service company – which was partly owned by the Portuguese government (in a partnership with Altice and Motorola) – was recently bought back by the Portuguese state for €7M. The system is estimated to have cost upwards of €450M to install and manage thus far. This came after numerous operating issues were detected that hindered the private sector's positioning in the company. Even so, the Portuguese government still pays Altice and Motorola €30M a year to operate and rent out the network. A recent study points to the costs of implementing robustness and security improvements in the network to be upwards of €25M, which currently consists of 550 antennae, all across national territory. This points to the significant costs of installing, maintaining and operating the infrastructure, which are still significantly lower than the cost of operating a large consumer-grade system. In particular, the costs associated with a complete replacement of the system if a malicious vendor is detected within its confines can be extrapolated to be close to or higher than the costs associated with installing and maintaining the system over the past 15 years of operation.

# Summary & Conclusions

Depending on the subject and cost category looked at, we estimate the annual hidden costs of failing to exclude untrusted vendors as ranging from €19M for the operation of a test centre, to more than €388M Euro for a shift of demand of IPR and critical infrastructure industries. This is not to mention the drastic cost to the economy of a total shutdown as caused by a kill-switch Armageddon scenario. While some of these might only be used once (causing a rip-and-replace reaction by MNOs and regulators), they are not mutually exclusive.

What this country study illustrates, particularly in the context of the larger policy paper implications, is that even if there is some cost to slightly delaying the rollout of 5G infrastructure, or to choosing a marginally more expensive vendor, the systemic risks and costs of a potentially untrusted alternative is indeed quite large.

Portugal is yet to complete the 5G auction and the overall regulatory picture around its 5G network requirements. The EU Toolbox and its recommendations will undoubtedly serve as a template for policy-making in the country, but the decisiveness with which it is applied will determine its overall efficacy. If we look at the examples of other European countries who have recognised these risks and taken action, we will see the importance of making prompt and uncompromising decisions that not only safeguard the free market by protecting its fairest actors, but also adopt a long-term view of the consequences of failing to do so on national security and the European economy.

In recent years, Portugal has seen its secure communication networks failing in critical conditions, absorbing considerable political and societal implications as a result of highly publicised data breaches, suffering through high-impact strikes. It has seen cybercrime statistics rise well above global average, and so understands very well the impact of well-designed regulation and procurement processes on its growth potential.

There are also the non-monetary costs, such as the potential unwillingness of allied intelligence services to share security-related intelligence with the Portuguese government, if that intelligence could leak out for technical reasons. There is still plenty of time for Portugal to lead in this regard and ensure the long-term success of its 5G rollout program.

In conclusion, we have been able to show that the total societal costs for Portugal, 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. This form of market failure must be overcome through adequate regulation in order to fully realise the growth-enhancing potential of 5G. In the following picture, we summarise the costs per category, as described in this country study.