BIGS | Policy Paper

Brandenburg Institute for SOCIETY and SECURITY

BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

The Hidden Costs of Untrusted Vendors in 5G Networks

Stuchtey, Dörr, Frumento, Oliveira,
Panza, Rausch, Rieckmann, Yaich

BIGS Policy Paper No. 8 / December 2020

Version v3: first published Jan 26, 2021; revised Feb 11, 2021.

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.

BIGS | Policy Paper

Brandenburg Institute for SOCIETY and SECURITY

The Hidden Costs of Untrusted Vendors in 5G Networks

Tim Stuchtey, Christian Dörr, Enrico Frumento, Carlos Oliveira, Gianmarco Panza, Stefan Rausch, Johannes Rieckmann, Reda Yaich

December 2020

Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH
Brandenburg Institute for Society and Security gGmbH

Executive Director
Dr. Tim H. Stuchtey

Dianastraße 46
14482 Potsdam

Telephone: +49-331-704406-0
Fax: +49-331-704406-19

E-Mail: direktor@bigs-potsdam.org
www.bigs-potsdam.org

PREFACE

All across Europe, countries are talking about 5G. Central to the ongoing discussions are the economic opportunities offered by this new mobile communications standard, the potential leaps forward in productivity, the vulnerabilities associated with stronger networking, and the dependencies that would result if these new networks were built using Chinese technology. On another occasion, Director of the Hasso Plattner Institute Christoph Meinel and I termed the latter prospect the "Huawei shock", in reference to a historical moment with parallels to the present: when the Russian Sputnik missions succeeded in shaking up the West. Following the many recent discussions concerning 5G, some governments have excluded Chinese network providers when setting up domestic 5G networks, or have implemented regulatory hurdles in such a way as to result in a de facto ban.

Countries expect a high degree of trustworthiness from those providing 5G, given that it is a supercritical infrastructure of the future. 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. These criteria are difficult for Chinese competitors to meet because they are headquartered in a country with a managed state economy that requires unconditional obedience from companies, that has a terrifying record in terms of the rule of law, and that, according to western intelligence services, cybersecurity companies and many media reports, is the origin country of many attempts at industrial espionage.

If companies with such origins are nevertheless to play a role in setting up 5G networks in Europe, considerable costs can be expected. Only some of these costs are incurred by the mobile network operators, who are – absent any further regulation – free to make their own decisions about their network providers. But many of the costs will be borne by other sections of society, such as telecommunications customers or taxpayers, who, without further regulation, have no input on the selection of network equipment provider. Additionally, some of these costs will only be incurred long after the network has been set up, leading to a risk that these costs will not be adequately taken into account in the initial investment decision.

In this study, we reveal the hidden costs of these untrustworthy network vendors and, insofar as possible, calculate the costs more precisely for four European countries (Germany, France, Italy, and Portugal). To tackle this challenge, we assembled an esteemed interdisciplinary project team, already largely familiar with one another from previous European research projects. We have been working closely on this issue since the summer, despite many degrees of geographical separation. Plans for meetings in Aveiro, Berlin, Milan and Paris unfortunately fell victim to the COVID-19 pandemic. Nevertheless, we were happy that our project was interrupted only by two births and not by a contraction of COVID-19.

We would like to thank the many experts, colleagues, and external employees of our institutions who supported us in various ways while preparing this study. Particular thanks go to the US Department of State, which made this study possible through its financial support. The authors are solely responsible for possible errors in our argumentation or calculations. We hope that, with this study, we can make a constructive contribution to decision-making in our respective home countries.

Dr. Tim H. Stuchtey

December 2020

EXECUTIVE SUMMARY

While a 5G symbol can already be seen on cell phone displays in some European metropolitan areas, most networks are still in their planning phase. Firstly, mobile network operators (MNOs) must decide from which vendor they wish to procure the network technology. In many cases, it seems that MNOs want to build the networks at least partly using technology from Chinese manufacturers, assuming that government regulation or their customer base do not demand otherwise.

In this paper, we explain why the security of 5G networks is of greater significance for the economy than was the case with 4G. We outline the costs associated with building networks using untrusted technology, and try to measure those costs where possible. We include country studies for our home countries Germany, France, Italy and Portugal.

Chinese vendors are considered untrusted because they operate from a country with strict government controls of their business and management, and that lacks sufficient rule of law. A dearth of trust in the vendor of 5G network technology must be compensated for with greater control over the network or the data running through it. Because of continuous updating of the 5G networks, these control costs occur throughout the network's entire lifecycle.

MNOs do not take all costs into consideration when deciding from whom they wish to procure 5G network technology. This is due to the hidden costs that occur later in time (**lifecycle costs**) or because they are borne by someone other than the MNO (**external costs**).

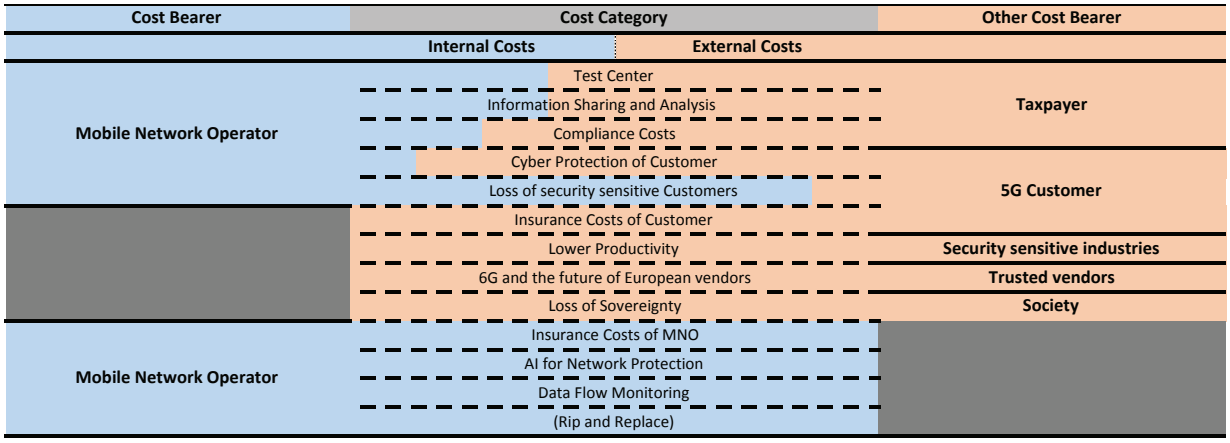
Some costs identified also occur when 5G networks are built exclusively with trusted technology. However, these costs will ultimately be lower because a trusted vendor can and will cooperate with MNOs and Western Governments to secure the network from external influence.

The hidden costs defined in this study can be divided into lifecycle costs and external costs, as demonstrated by the following table. Some costs are both external and occur later in the lifecycle. The external costs borne by somebody other than the MNO are also identified in the table.

When untrusted vendors are part of a 5G network, additional efforts must be taken to test and screen software updates provided by the vendor. Issues with the network caused by the network technology should be shared with other MNOs, government entities in charge of network and cybersecurity, and sometimes customers. New information sharing and analysis centres (**ISAC**) must be established domestically and at an EU level. Additional sensors must be built into the network in order to **monitor** network traffic and to recognise unintended dataflows to third parties. New **AI** tools must be developed and integrated into the network management as an early warning system for covert data exfiltration. Governments, MNOs and their customers will have to spend resources formulating, influencing, and enforcing **regulation** policy and compliance with it in order to compensate for the lack of trust in the network. In order to cover damages caused by cyberattacks enabled by 5G networks, the MNOs and their customers will have to spend more on cyber insurance to deal with the financial consequences. Customers that are, or have to be, particularly wary of data protection will refrain from using networks with untrusted vendors and shift their business elsewhere. In the case that an untrusted vendor's reputation is damaged because of additional evidence of collusion with state-sponsored cybercriminals, the untrusted technology will need to be replaced rapidly, including temporary network shutdowns, thereby incurring significant costs (**rip and replace**).

If the 5G network includes untrusted technology, a greater burden to protect the data of machines controlled through the network falls on the customer.

Table 1: Nature of hidden cost categories – external and lifecycle costs



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

Source: own Diagram.

They will have to spend more resources on cybersecurity tools, or refrain from using the network, thereby leaving potential productivity gains unused. European vendors will struggle to compete with companies that don't need to earn a profit from their 5G business. Even if these vendors remain in the 5G business, they will lack sufficient resources for R&D, particularly when it comes to developing the next generation of mobile networks for the 2030s (i.e. **6G**), in which case the West would be fully dependent on Chinese network technology. Governments whose economies depend upon the functioning of untrusted networks will think twice about challenging China in international disputes. Their political room to maneuver will be severely limited.

In order to internalise the external costs and the additional protection necessary, regulation is necessary to either rule out untrusted vendors from building 5G networks, or to require from MNOs investment in the additional protections necessary when using untrusted technology. Even though it is not possible to know if and by how much untrusted vendors are really offering their technology for less than trusted competitors in the four countries we analysed, the additional costs associated with the additional protection required, plus the external costs, will most likely outweigh any cost advantage offered by the untrusted vendors.

TABLE OF CONTENT

LIST OF FIGURES AND TABLES

1 INTRODUCTION

5G is considered a transformative technology that will soon be the basis of a high increase in productivity. 5G networks have started becoming available in several countries and are initially offering substantially higher download rates than 4G/LTE. In the future, however, further services will emerge from this new generation of cellular systems due to increased capacity, high speeds and low latency. Many existing industries will digitalise an increasing share of their value chain and run production and services over these mobile networks, thereby making 5G networks a quasi-supercritical infrastructure.

There is a saying among security researchers: if an innovative technology is not first abused by crooks, it's probably not that innovative. Connecting evermore aspects of our lives and businesses to the internet means that billions of new attack vectors are opened up for malicious actors. At the same time, our society is becoming more dependent on the integrity and availability, as well as the confidentiality, of these new networks.

The equipment required to build these networks comes from a handful of companies. Following a brutal phase of consolidation in the network industry, there are now five relevant suppliers on the market: Huawei, Ericsson, Nokia, ZTE, and, as a bit of a newcomer, Samsung. These companies supply the technology for mobile networks that are operated nationally by even fewer primary mobile network operators (MNO). These MNOs are assigned the relevant frequencies for their operation by their governments. In most countries, these frequencies were auctioned off by the state in bundles and bought by the telco operators, which then procure the network technology to make them serviceable.

If all five mobile network vendors provide the same functionalities and services, basic economic theory suggests that, all else being equal, the price of network equipment should be the same from vendor to vendor. In reality, however, Chinese vendors seem to offer their product at a significantly lower price than their western competitors. In some cases, the price is so low that it, presumably, fails to even cover the costs of production. This gives rise to questions about the rationale behind such offerings, such as why these companies are not behaving as private, profit-maximising firms typically do.

For the network provider, the initial costs of building the network are just one of many expenses. Since frequent upgrades and replacements of the network's hard- and software will be necessary throughout the lifespan of a 5G network, lifecycle costs are actually more relevant than the initial acquisition costs. It is also possible that not all costs associated with building, maintaining and operating the mobile network are borne by the operator. These costs must also be taken into account when making decisions about acquisition. Some costs might be external costs, which arise when producing or consuming a good imposes costs upon a third party. If there are negative externalities associated with providing a 5G network, the social costs will be greater than the private costs of the network operator. The following economic analysis will hopefully contribute to the debate.

Because of the supercritical nature of the 5G networks for our economy and society in the coming years, functionalities and service prices are not the only aspects that must be considered when choosing a network vendor. In order to ensure the confidentiality and integrity of the network and the data within, it is critically important that the mobile network operator has a comprehensive understanding of what its network does and has full control over the network traffic. In the case that they fail to do so, they become financially, or at least politically, liable for the damage enabled by their network.

With 5G networks, many functionalities that were implemented on ad hoc hardware in past network generations are now realised through software running on general purpose hardware. In the near future, these will also be realised on open platforms. Software must therefore be updated on an ongoing basis in order to offer greater functionality over time.

The billions of lines of code that create a network cannot be fully understood and controlled by the network operators. Even government entities and large research institutes can replicate this only for parts of the network. Consequently, network operators and customers must trust the network vendors that their equipment performs only what it should and nothing more. They must also trust that no one other than the network operator controls the network. When trust in the vendor isn't sufficient, trust in the legal system and in the financial liability of the vendor should act as a safety net.

Trust is hard to measure, but the rule of law in a country can at least be a measure for the proper functioning of a legal system and the possibility of enforcing financial claims. Among the five companies offering 5G networks, three are based in countries in which the rule of law is ranked among the highest in the world according to the World Justice Program's 2020 Rule of Law Index:[1] Finland (#3), Sweden (#4), and the Republic of Korea (#17). Two vendors come from China, which is ranked 88 out of the 128 countries ranked. China does particularly poorly in this ranking with regards to improper government influence on the civil justice system (#122), constraints on government powers (#123), and fundamental rights (#126).

Consequently, Klas Friberg, head of the Swedish Intelligence Service, has stated: "The Chinese state carries out cyber espionage in order to promote its own economic development and to develop its military capability. It does so through comprehensive intelligence collection and theft of technology, research and development. This is something we have to take into account as the 5G network is being built. We cannot make compromises when it comes to Sweden's national security."[2]

Similar comments have been made by several other European intelligence officials. Furthermore, CrowdStrike, a US cybersecurity technology company, identified China as "the most prolific nation-state threat actor during the first half of 2018."[3] Former US Assistant Attorney General John C. Demers stated at a Senate hearing that, from 2011-2018, China was linked to more than 90% of the US Justice Department's cases involving economic espionage and two thirds of its trade secrets cases.[4]

It would therefore be naïve to believe that implementing a technology with so much opportunity for undermining the integrity and confidentiality of data, as well as the possibility for brute sabotage by untrusted vendors, would not come with hidden costs. In this study, we will try to name these costs, define them and to measure – or rather, estimate – them for France, Germany, Italy and Portugal. By doing so, we hope to provide those in charge of procuring 5G technology and those who regulate the market with additional insight to inform their decision-making. This insight should also better enable them to follow the advice of Chinese President Xi who, when speaking at an internet conference, said "we should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation, and internet public policies, and participate in international cyberspace governance on an equal footing."[5]

Readers who are already familiar with 5G and its impact on the economy, and who possess basic understanding of how 5G operates technically, can skip Chapter 2. Those who understand the importance of trust in the functioning of technology (Chapter 3) and the security impact of 5G (Chapter 4) can jump straight to the chapters about the obvious (Chapter 5) and the hidden (Chapter 6) costs of untrusted vendors in 5G networks. In Chapter 7, we describe the costs that would incur should apprehensions about untrusted vendors be confirmed. We conclude with three scenarios and their economic consequences before seeking to apply this framework to four countries: France, Germany, Italy and Portugal.

1 World Justice Report (2020).
2 Säkerhetspolisen (2020).
3 Crowdstrike (2019).
4 Demer (2018).
5 Xi (2015).

2 WHY IS 5G IMPORTANT?

The first generation of wireless cellular[6] 1G, first launched in Japan in 1979, offered analogue voice services, while 2G, launched in 1991, replaced that with digital voice and SMS (text) services. 3G, launched in 2001, offered sufficient data rates for the first truly effective mobile internet services. 4G, introduced in 2009, was built from the ground up for fast mobile internet, facilitating the smartphone revolution and app economy (see Table 2 below).

With the transition towards large-scale deployments of the omni-connected Internet of Things (IoT), these existing mobile communication networks are no longer sufficient. Forecasts predict that the number of worldwide networked devices will grow to 55 billion by 2025.[7] These devices will be rolled out in agriculture, manufacturing, health and environment-sensing applications, but will also enable new services and applications in transport, such as self-driving cars. This drastic increase in devices per square kilometre and the emergence of new services with different bandwidth and latency requirements, as well as the omnipresence of machine-to-machine communication, cannot be realised by the existing 4G infrastructure.

5G is thus not merely an evolution towards more bandwidth, but a paradigm shift in how mobile communication networks are built. The key innovations of 5G happen not only at the edge of the network, where the connection is made between mobile handset and cell phone tower, but largely at the core and management level. In the following sections, we will briefly discuss the new value propositions, the resulting requirements, and the high-level design of a 5G network.

Table 2: Evolution of mobile networks – up- and download speeds

	1G	2G	3G	4G	5G
Approximate deployment date	1980s	1990s	2000s	2010s	2020s
Theoretical download speed	2kbit/s	384kbit/s	56Mbit/s	1Gbit/s	10Gbit/s
Latency	N/A	629 ms	212 ms	60-98 ms	< 1 ms

Source: ITU 2018, p. 6.

2.1 New Use Cases

Compared to 4G, 5G offers 10 to 100 times the data transfer rates, only one tenth the latency (the 'lag' time taken for devices to communicate with each other), far greater bandwidth, and 10 times the number of connected devices in a given territory (see Table 3). In addition, the technology is more energy efficient per bit of data transferred.

6 Cellular networks are formed of many transceiver antennas which each create a communications 'cell' around them for phones and devices to connect to. Replicated many times across a landscape, they provide ubiquitous, seamless coverage for connecting devices.

7 IDC (2020). https://www.idc.com/getdoc.jsp?containerId=prAP46737220#:~:text=IDC%20predicts%20that%20by%202025,from%2018.3%20ZB%20in%202019

Table 3: Technical Characteristics and Benefits of 5G Compared to 4G

	Latency	Peak data rates	Download speeds (Mbps)	Connections/ km2	Available spectrum	Illustrative antenna coverage (km)
4G	10ms	1Gb/s	1000	100k	3 GHz	50-150 (Mobile) 1-2 (Fixed wireless)
5G	<1ms	20Gb/s	10000	1m	30 GHz	50-80 (Mobile) 0.25-0.30 (Fixed Wireless)

Source: Kim (2019) and Singaligum (2019)

5G opens the door not only to better mobile communication services for individuals and enterprises, but for the connection of millions, if not billions, of machines – the explosion of the Internet of Things in different settings (see Figure 1 below). The International Telecommunications Union (ITU) has identified three game-changing, generic use cases:

- **Enhanced mobile broadband (eMBB).** An evolution of the primary use of 4G made possible by its higher speeds. 5G will allow "enhanced indoor and outdoor broadband, enterprise collaboration, and augmented and virtual reality", typically for individuals.

- **Massive machine-type communications (mMTC).** A new use case. The high bandwidth of 5G will allow for millions of sensors and machines to connect and pool data with each other and with the organisation that owns them. This enables far greater efficiency and efficacy of services, enterprises, and even 'smart' infrastructure. Applications include significantly more efficient and responsive logistics, transport hub operations, traffic flow management and electric grid control.

- **Ultra-reliable and low-latency communications (URLLC).** The very low latency offered by 5G makes it possible for sensors and machines operated by organisations wanting to provide time- and safety-critical applications to be connected, and allows them to work together for the first time. Applications include autonomous driving, remote medical surgery and management of critical national infrastructure.[8]

5G has benefits for, and will greatly benefit from, other areas of technology and innovation also currently underway. According to the ITU, 5G is one of five pillars of the digital transformation, along with the IoT, alternative/virtual reality, cloud services, and artificial intelligence (AI). With regards to AI, for example, 5G will greatly increase available sensors, providing massive amounts of data crucial to the training of machine-learning algorithms at the heart of AI-powered systems. With new sources of data come new opportunities for new AI-based services and business models to emerge.[9]

This means we are likely to see groundbreaking new areas of benefit and productivity growth for businesses and society emerging around 5G:

- Intelligent transport: 5G vehicle connectivity enables vehicles to connect to each other, to the infrastructure, to network services, and to other road users. This may lead to more efficient and safer road use. 5G makes possible truly automated vehicles.[10]

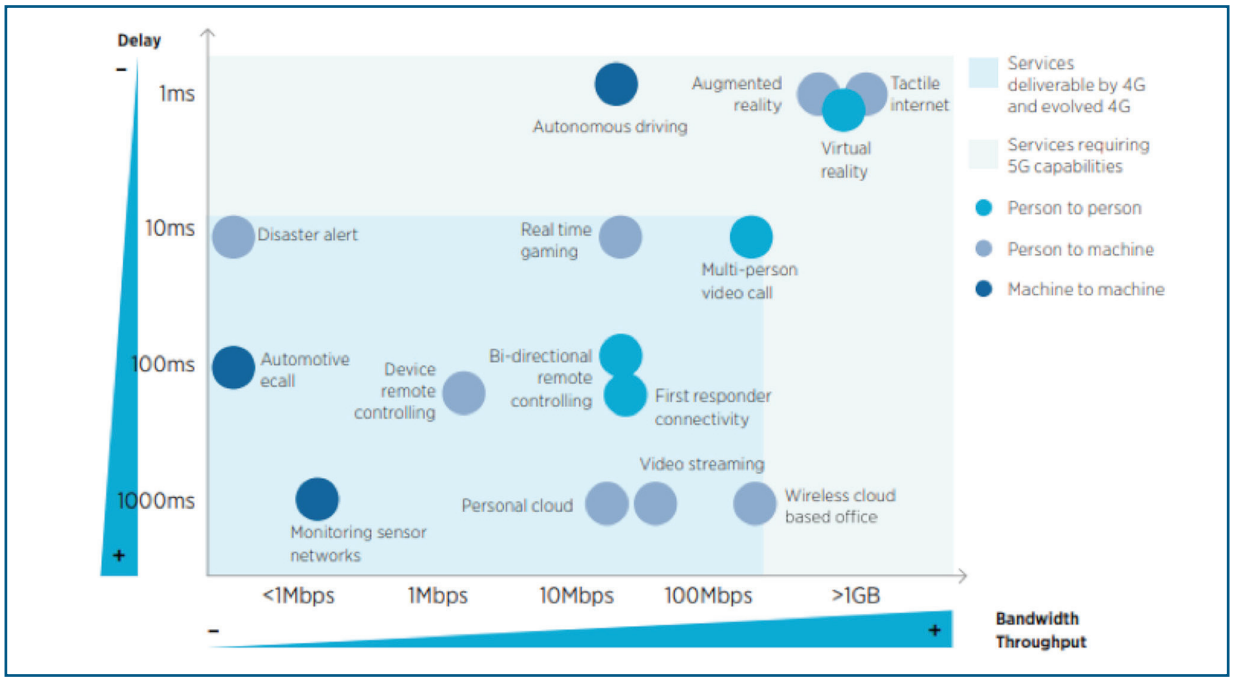
- Smart cities: As the key enabling technology for the IoT involved in management of urban transport systems, energy grids, and municipal services, 5G makes possible the vision of 'smart cities'.[11]

- E-health: High-resolution video consultations, assistance robots for surgery and smart wearables, such as joint implants, could all help to increase the efficiency and effectiveness of treatments, changing the places in which treatments are possible, as well as helping healthcare to shift towards more preventative interventions.[12]

8 ITU (2018), p. 6.
9 Taulli (2020).
10 Nokia (2020a).
11 Behesti (2019); Hui et al. (2020).
12 Nokia (2020b).

- Industry 5.0: 5G will drive the transition from Industry 4.0 to 5.0, a revolution focused around cooperation between machines and human beings, with the aim of providing added value to production by creating personalised products able to meet customers' requirements.

Figure 1: 5G will support low latency and high throughput throughout Services



Source: GSMA (2019), p.31.

In economic terms alone, the benefits will likely be huge. By some estimates, 5G will underwrite USD 12.3 trillion of global economic output by 2035. Investment in the 5G value chain is expected to generate a further USD 3.5 trillion in output and provide support for 22 million jobs by that point.[13]

5G is also likely to play a key role in security and defence in the future. Commentary on the impact of 5G for law enforcement and intelligence services is limited, but we can already find examples of 5G infrastructure helping law enforcement to precisely locate individuals and missing persons,[14] and becoming useful for the emergency services, from the control room to the frontline.[15]

For the military, the benefits of 5G are more obvious. According to NATO analysts, the alliance must exploit 5G technologies for command and control, communications, and other military purposes. They note that, without 5G, it will be difficult to fully exploit big data, artificial intelligence and cloud computing on the battlefield.[16] The US military is already pressing ahead. They have recently announced USD 600 million in funding for 5G experimentation at 5 different military bases.[17] As the

13 ITU (2018), p.8.
14 Roke (2020).
15 TechUK (2019).
16 Gilli and Bechis (2020).
17 The Hill (2020).

US Department of Defense Strategy on 5G notes:

"Ubiquitous high-speed connectivity will … transform the way militaries operate … the deployment of 5G capabilities will offer a host of opportunities to both reform DoD enterprise services and to create powerful new military advantages." [18]

Security and defence impact will be complicated by the extent to which law enforcement, intelligence services, defence and critical infrastructure providers are divided between proprietary and public 5G networks, something which is difficult to forecast. The vulnerabilities and dilemmas that 5G may create is the subject of the next section.

2.2 5G System Requirements

These new application scenarios for the fifth-generation mobile network create a number of new technical requirements. In order to meet these, 5G networks rely, on the one hand, on evolved and upgraded technology components, but also follow a different design paradigm. In the next section, we will briefly discuss which technical requirements are created by these use case requirements from the perspective of the system and its management. In the following section, we will discuss how these are realised within the 5G ecosystem.

1. **High data rate and low latency:** As shown above, every new generation of mobile networks has provided a significant increase in maximum and sustained bandwidth to the end user. While 4G networks can provide peak data rates of 1 Gbps and sustained experience bandwidth of around 10 Mbps, new services such as autonomous driving or virtual reality will greatly exceed what can be reliably provided by current networks. Within 5G, the experienced data rate is expected to increase one-hundred fold and reach up to 20 Gbps. Frequently these applications also have intense demands on data delay: for example, in autonomous driving where data must be shared across devices, latencies of 1 ms are a target, which is one tenth of what is provided by current mobile networks.

2. **Massive connectivity:** Each connected device is provided with a slice of the connectivity available to the base station, both in terms of a small time slot as well as a part of the frequency spectrum. Until now, the network was mostly used by cell phone users and only a share of the net was used for machine communication. Previous generations of mobile networks were designed for a limited number of such slots, which are greatly exceeded by the new use cases and the proliferation of the Internet of Things connected by mobile networks. The new design of 5G accounts for these new use cases by increasing the number of connectable endpoints per square kilometer by more than a factor of 100.

3. **Energy efficiency:** While in previous mobile applications used by cell phones or mobile end points such as car uplinks, energy consumption was of lesser priority, this will change as focus shifts to the interconnection of the Internet of Things. In this new scenario, low-cost devices are deployed across wide areas, which means that these units must operate on battery power for extended periods of time, as servicing and replacement of batteries in the field is neither economically feasible nor ecologically viable. 5G will drastically reduce the energy consumption for the mobile unit, enabling sensory applications lasting 10 years or longer on a battery.

4. **Programmability:** With the 5G network infrastructure aimed at supporting a variety of services with different performance requirements, the system architecture is based on flexible building blocks that can be individually programmed. This can take place at different layers: services are compartmentalised and can obtain different data allocations and security levels. For instance, an eHealth application can be operated in an entirely different zone, interference free from normal cell phone usage. This isolation of different use cases allows for services with strict quality requirements can be accommodated.

18 Department of Defense (DoD) (2020).

Foto © AerialPerspective Works/iStockphoto

2.3 Components of a 5G Infrastructure

To enable these new applications and realise their requirements, 5G introduces a number of innovations in the Radio Access Network (RAN) and the network core. In the following section, a selection of these technological advances will be briefly discussed:

- The 5G **Radio Access Network:** The RAN refers to the part of the mobile network that interacts with the mobile users, the most visible component being the mobile base stations. To enable the high-bandwidth, massive deployment use cases, 5G networks make use of a larger frequency band, and particularly higher frequencies, than current 3G/4G installations, as high data rates can be more efficiently transmitted at higher, so-called millimeter wave frequencies. Network capacity and density is further increased by the use of MIMO (multiple input, multiple output), which means that multiple antennae are used at the same time to transmit and receive data to a single mobile device. 5G relies on massive MIMO — thus many different antennae for different users — and beam forming to increase the throughput on the radio interface. As radio spectrum — in other words, communication frequencies — is a limited and expensive resource, 5G further increases the number of users and devices it can support by increasing the density of cells. With each operated by low-powered radio access nodes, this allows the network operator to reuse the same frequencies over a larger area, as transmission power and thus potential interference is reduced. Low transmit power also results in energy savings and better battery runtime.

In addition to these improvements, which happen at the interaction between the mobile base station and the subscriber's device, there are also major changes in how the hardware operates in the RAN. Instead of dedicated hardware that encapsulates all the functionality, innovations such as cloudRAN now decouple the remote radio head — simply put, the transmitter/receiver of the cell phone tower — from the base unit, which carries out the signal processing. Both are linked by high-speed fiber networks and enable the mobile network provider to operate the latter within a cloud computing environment. This means that networks can be more easily scaled with increased demand, and no longer rely on specialised hardware, making them cheaper to operate. With

the very high requirements on bandwidth and latency of new 5G services, these service requirements can only be met by moving services closer to the mobile user. This is referred to as edge or fog computing and is made possible because many services can be provided through virtualisation on the same system hardware.

It is sometimes argued that RAN is a relatively insignificant part of a 5G network and that it cannot affect the confidentiality and integrity of 5G services. However, from a technical point of view, this argument is mistaken. The 5G base station (gNB) is the end point for encryption and integrity protection. Therefore the user layer is potentially accessible (to anyone having access to the base station) in clear text if no end-to-end encryption is used.[19] In this context, the technical aspects of security in RANs are as critical as the core network in terms of integrity and confidentiality.

- The 5G **Core Network:** As the network must provide multiple services with different service requirements concurrently, 5G realises this co-existence and flexibility through the use of **programmable networking.** Software defined networking (SDN) is an established technique in data centre networks and is used in the context of 5G to accomplish an agile core, which can be adapted to new requirements and newly introduced services. This makes it possible for network operators to deploy additional services with minimum effort. A similar **softwarisation** is provided by network function virtualisation (NFV), where network functionality is no longer provided by means of specialised, dedicated, and thus expensive, hardware, but through software on commodity servers that make it easier to scale with changing demand and implement new functionality in faster deployment cycles at greatly reduced costs.

5G leverages these technologies to implement **network slicing**, where the same physical hardware is split into multiple logical compartments, each dedicated to different end users (e.g. autonomous driving, eHealth, personal cell phones) with different performance and security demands. This guarantees complete interference-free separation of different applications and use cases on the same hardware, thus saving costs, and allowing networks to create mobile virtual network operators (MVNOs) much more easily than before.

To leverage the full potential promised by 5G, both an upgraded radio access network (RAN) and an upgraded core network are necessary. At the moment, there exists almost no mobile network worldwide that is "fully" 5G: in other words, where all required components are deployed in both core and RAN. Most networks have begun to implement an improved radio access network, where massive MIMO or smaller cells can already provide improved user bandwidth compared to 4G/LTE technology, but do not yet enable the different application scenarios possible within an "all-5G" network (see Table 4).

Table 4: System requirements from use cases and technical realisation in 5G

System Requirement	Technical Realisation in 5G
High data rate, low latency	Massive MIMO, Smaller Cells Edge Computing
Massive connectivity	Massive MIMO, Smaller Cells
Energy efficiency	CloudRAN, Smaller Cells
Programmability	CloudRAN, SDN, NFV, Network Slicing

Source: own Diagram.

19 See Ericsson (2020a).

3 WHY IS TRUST IN 5G NETWORKS IMPORTANT?

Across society as well business, trust is fundamental: without it, people can neither act nor interact. It is no surprise that Abraham Maslow situated trust on the second layer of his hierarchy of human needs, just after the physical requirement for human survival. In the IT-/cyber industry, we often hear the slogan: **security builds trust and trust builds business.** With this in mind, how can telecom providers presume to do business successfully if trust in their network is lacking?

As critical as it is, trust is hard to define and quantify, even harder than security. In economic terms, trust means a reduction of transaction costs. Because of trust, we let our guard down and spend less on control and protection. Gambetta defined trust as *"a particular level of subjective probability with which a party A expects that another party B performs a given action, both before it can monitor such action and independently of its ability to monitor it."* [20]

In a few short years, fifth-generation networks will constitute the backbone of our societies and economies, linking billions of objects and systems, including those used in critical sectors such as energy, transport, healthcare, banking and industry. When a network with such enormous impact on our society and economy is built and maintained (in part) by companies from countries with weak rule of law, where basic democratic principles are openly violated and where intellectual property rights are disregarded, it is hard to build trust. "Trust but verify" isn't just a proverb, meaning lack of trust must be compensated for by increased efforts for protection and control.

Trust concepts, as they are now understood, are not sufficient to manage complex 5G infrastructures. Trust in 5G vendors can have a variety of foundations. Trust can be founded on the quality of a vendor's products, on a long-term relationship, or on the vendor's reputation. The ability to verify the content (hardware and software) of the vendor's equipment is also often used as a basis for trust. As 5G networks will be largely Software Defined Networks (SDN), which reduce the operating and maintenance costs for the MNO and will be incomparably more dynamic than 4G networks due to software patching and updates, it will also become increasingly difficult – if not outright impossible – to vet each adjusted software version and component on a continuing basis effectively, efficiently and in time. In a competitive and profit-oriented environment, therefore, vetting will have to be done selectively, while a significant share of software adaptations will have to be trusted due to time, budget, personnel and other resource constraints.

In many ways, the market for 5G network hard- and software can be described as what George Akerlof called a **"market for lemons"**, meaning a market in which the buyer cannot distinguish between more secure and less secure network vendors. There is an **information asymmetry** between the two sides of the market.[21] Buyers don't know when they commit to a vendor if they will get a peach (good quality) or a lemon (low quality). If buyers simply assume that all vendors offer the same average level of network security (trust every vendor), the result will be that demand will lean towards the supplier with the lower price and lower security quality. Ultimately, the higher quality and more secure vendors will leave the market, resulting in an **adverse selection towards low security** networks, with huge consequences not only for the 5G market and its applications, but also for the next generation of mobile networks (6G).

Trust is also important in the market for 5G services, where the mobile network operators are the suppliers and demand comes from companies, government and citizens. Customers will have little to no knowledge about the inner workings of a 5G network, and again we will witness a great deal of information asymmetry. Customers will have no choice but to trust the MNOs and will afford them **goodwill** earned through past performance. However, this goodwill can easily be lost if suspicions occur that the trust is not deserved – and while for an operator, regaining trust is costly, customers can switch network providers with minimal effort.[22]

20 Gambetta (1988), p. 216.
21 Akerlof, George A. (1970).
22 For a more in-depth discussion of the role of trust inn cybersecurity see Lysne (2018), p. 11 ff. Olav Lysne, The Huawei and Snowden Questions, Simula SpringerBriefs on Computing, Vol 4, Springer 2018. https://www.springer.com/gp/book/9783319749495

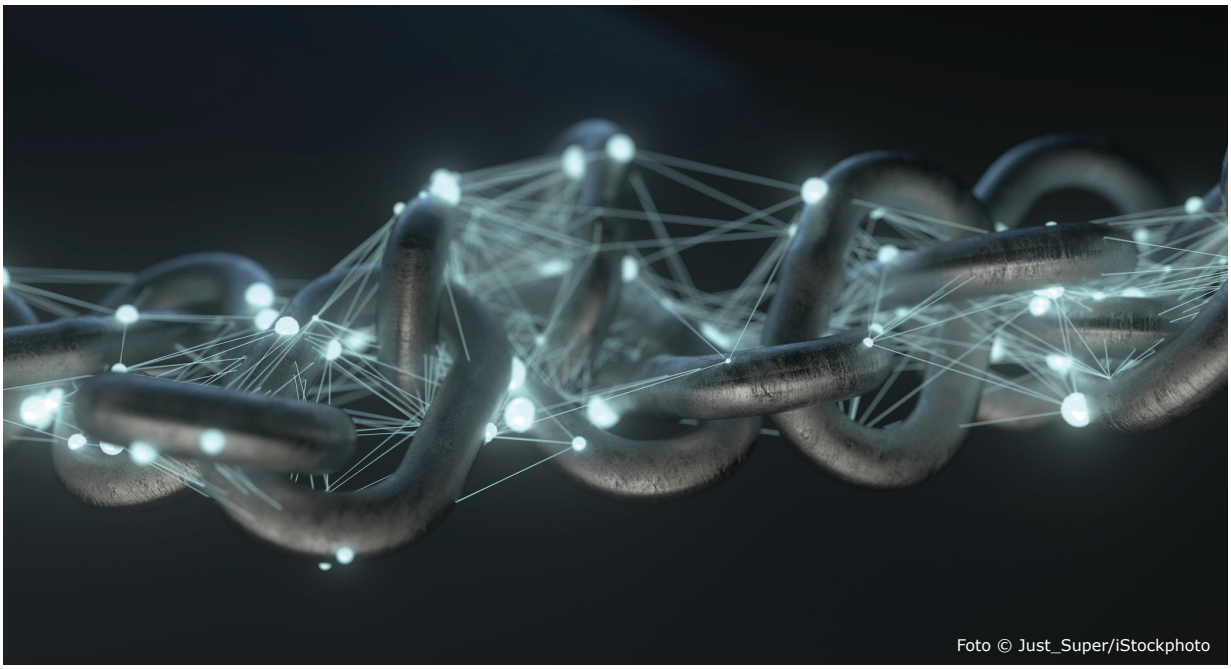


Foto © Just_Super/iStockphoto

4 WHY IS 5G SECURITY RELEVANT?

No communication technology is ever completely secure, and 5G is no exception: it presents significant new vulnerabilities and challenges.[23] What makes 5G qualitatively distinct from previous generations of telecommunications technologies is that it is becoming a new 'supercritical national infrastructure' upon which key parts of the economy and national infrastructure (such as water supplies and electricity) depend.[24] It also makes up part of the infrastructure over which vital future communications for economic health and national security will take place. A cyberattack on power grids would, for example, be devastating.[25] Hackers are already adapting their craft for the possibilities of 5G.[26] It is therefore extremely important that states consider security before making major decisions on 5G.

Information security consists of three elements, sometimes referred to as the **CIA triad**: confidentiality, integrity and availability. The focus of the protection mechanisms in classical office IT and in industrial research and development was previously on the protection of confidentiality. However, with the rise of Industry 4.0 and the Internet of Things, fueled by the evermore rapid networking and automation of production plants enabled by 5G infrastructure, the importance of the other two security objectives, integrity and availability – which form the thrust of sabotage activities – becomes increasingly clear.

Confidentiality means limitations on access and restrictions on information. Confidentiality is broken in the context of industrial espionage or for other reasons for eavesdropping. It is often affected by infringement of intellectual property (IP) or privacy. Besides competitive disadvantages arising for the owners of IP, liability questions arise. Is the MNO liable or at least politically held responsible for IP theft and privacy violations? As the value of data/

23 For an overview of the 5G security risks see for example 5G PPP Security Working Group: Phase 1 Security Landscape. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf
24 Cave (2020).
25 Lloyds (2015).
26 Wheeler (2019).

information increases in a digital economy, so does the value of confidentiality. If property rights to information cannot be guaranteed, it means that access to this data is not fully controlled. Confidentiality is also of major importance in the field of national security. Sharing of intelligence among allies is jeopardised when at least one government relies on insecure communication technology.

Integrity relates to the risk of content manipulation. Malicious modification of data corrupts datasets and can, for example, sabotage product quality in industrial 4.0 manufacturing, lead to errors in business decisions, disrupt warehousing and maintenance, and so on. If 5G-controlled factories allow an attacker to compromise the integrity of production, such a tool will much more elegantly destroy or hurt a competitor than a brute force disruption of the production. Or, from the viewpoint of the defender: it is good to know that the machines are running, but it is even more important to know that they are producing what they are supposed to produce.[27]

Availability in the context of a mobile network means, first of all, that the network is up and running. The network can also potentially be gradually curtailed by malicious parties. Temporary or local to regional slowdowns are conceivable,[28] and even severe interferences, including complete network disruptions (like flicking a kill switch), cannot be excluded in the case of escalating international conflicts. The latter is probably a rather unlikely event, as it would inevitably trigger a subsequent rip and replace scenario. An example of availability disruption is the 2007 cyberattack on Estonia, presumably by Russia. Since then, the dependency of our economies and societies upon digital networks has dramatically increased.

4.1 Technical Infrastructure and Future Scale of Reliance on 5G

As briefly explained at the outset, the causes of risks to the security of 5G are manifold, and include the technical infrastructure and associated applications creating more vulnerabilities and opportunities for attackers. While analysts disagree on the magnitude, many agree that 5G will present risks if implemented poorly. The European Union Agency for Cyber Security (ENISA) notes two key aspects of 5G that make it distinct from previous generations of wireless telecommunications technology: *"novel network technologies and concepts – heavily relying on 'softwarisation' and virtualisation of network functions – will introduce new and complex threats."* [29]

Compared to 3G and 4G networks, **5G networks are highly software-intensive**, with millions of lines of code responsible for the definition, management, and availability of network functions. Hub-and-spoke hardware-based switching has given way to decentralised software-defined digital routing, removing hardware 'choke-points' at which security inspection and control could take place. Management and Orchestration (MANO) functions, including security, are now performed almost exclusively at the software level, potentially leaving them vulnerable. Software for network slicing – dynamic creation and management of multiple virtual networks of different characteristics – could also be vulnerable to compromise, as cybersecurity standards fluctuate with the use case. As ENISA notes, virtualisation of hardware functions is commonly done through open-source software, protocols and systems – well understood tools available to all, including those seeking to do harm.[30]

The physical configuration of the infrastructure also introduces vulnerabilities. Physical assets at

27 Timo Kolb quoted in Bitkom 2018, p. 45.

28 In times of pandemic-related lockdowns, such impairments are particularly severe, since a considerable part of the professional work has to take place from home. Cf. Strand Consult (2020), p.3: „While trade disputes make for sensational news stories, it does not diminish the fact that countries increasingly view telecommunications as vital infrastructure requiring increased security, particularly in light of Covid-19 lockdowns in which people must work, learn, and receive healthcare from home."

29 ENISA (2019), p. 19.

30 Drawing on ENISA (2019), and Wheeler (2019).

the base of the network now perform so many tasks through overlaid software that the number of assets can be reduced, meaning a loss becomes more significant in the service provisioning chain. That said, the higher frequency bands of the 5G spectrum[31] are only available at shorter distances than 4G, necessitating the construction of many **more access points**. Each one of these 'access network' nodes is another point of vulnerability that connects back to the core network infrastructure.[32]

Moreover, the proliferation of connecting devices on 5G networks means there is a high chance that **insecure devices** will be present, and it will simply be impossible to police the security of all devices. Each device then potentially becomes an attack vector against other devices, or at least for an isolated segment of the network. Insecurities created by IoT devices, and by their manufacturers and users failing to secure them properly, are well-documented.

4.2 Security and the Choice of 5G Vendor

5G is built with equipment and software supplied by companies, and governments must decide which companies to entrust with the installation and management of telecommunications systems crucial to the future functioning of their country. Companies always operate from within a state jurisdiction and political system, and not all political systems align with the values and goals of western liberal societies.

In recent years, considerable suspicion has fallen on Chinese 5G vendors, who offer the most comprehensive 5G infrastructure of the competitors.[34] [35] Huawei's case has been most public. Chinese equipment will be phased out from telecommunications networks in the US, UK, New Zealand, and Australia later this decade. France, Germany, Italy, and Portugal are developing legislation that will require governments to consider both the technical and political reliability of vendors.

The technologies and networks themselves are too complex for security agencies to assure decision-makers that every component and line of code is free of bugs or 'back-door' vulnerabilities. Security agencies also point out that Chinese companies are dependent on legally mandated requirements for them to turn over information to the Chinese government.[36]

The **rule of law** in China on **privacy protection** is very vague. The term "privacy protection" was only included in Chinese laws and regulation in 2009, with several legal possibilities for the government to demand the handing out of data from the private sector.[37] For this reason, Chinese vendors do not have a solid legal basis to protect data from the Chinese government.

Considering where past acts of industrial espionage originated, we could question the rationale of **making the wolf the shepherd of the herd of machines**. Of course, in a liberal society, a company cannot be equated with the state from which it originates. But this is different in autocracies. As the German domestic intelligence service (BfV) clearly states in its annual report: *"Due to the close interdependence of state and economy in China, it is hardly possible in individual cases to differentiate between state-operated industrial espionage and spying by competing companies."*[38]

The BfV also states that cyberattacks on Germany from China are increasing: *"The core objective was primarily commercial enterprises. The attackers are presumably pursuing the goal of promoting selected Chinese economic sectors through industrial espionage and illegitimate knowledge transfer and thus supporting Chinese ambitions on the way to*

31 5G operates on three separate frequency ranges.
32 Drawing on ENISA (2019), and Wheeler (2019).
33 Drawing on ENISA (2019), and Wheeler (2019).
34 Lewis (2018), p.4.
35 Crawford (2020).
36 Draws on BfV (2019), Watts (2019), Lee (2019).
37 Wang (2017), p. 243.
38 BfV (2019), p. 294.

becoming the world's leading economic power. The framework for cyber-attacks is set, among others, by the current "Five-Year Plan", MIC 2025 and the BRI. The extensive industrial espionage and the targeted, systematic illegitimate transfer of knowledge through Chinese cyber-attacks cause significant damage to affected companies and the entire economy." [39]

Therefore, information security, as a triad of confidentiality, integrity and availability of data, is not ensured by 5G vendors coming from legal systems that do not relate privacy protection to the restriction of government power. The German Council of Economic Advisers states that China lacks transparency in their political processes and also has a high level of corruption.[40] In such an environment, **the dichotomy of the market and the state does not exist**, as government-owned and private companies alike need to maintain privileged relations to the Chinese government in order to benefit from economic surpluses.[41] As 5G is part of a debate on technological dependency and political sovereignty,[42] the question arises whether one should buy from vendors that do not follow a strict economic rationale, but are themselves dependent on an autocratic government.

Foto © Stefan Tomic/iStockphoto

It is likely that Chinese technology companies have already been used by their government for hacking against the West and surveillance of dissidents, particularly in countries with poor governance and weak rule of law.[43] The global political situation and China's related political and economic ambitions lead us to expect a further intensification of espionage and exertion of influence. In our view, it is naïve to assume that the opportunities for such activities that would arise from access to 5G networks would remain unused.

As noted above, the preeminent global militaries are already funding 5G technologies for dedicated military use in bases, command and control architectures, and battle networks.[44] States must also bear in mind that national security is frequently a collective enterprise, and considering the security of 5G now is necessary to prevent significant (political and economic) barriers to bilateral and multilateral collaboration emerging later. For example, it is unclear how far national security institutions will come to rely on *public* 5G networks, consciously or inadvertently. US concerns, expressed to European and 'Five Eyes' allies, rest on the argument that shared information will be vulnerable to Chinese espionage through untrusted Chinese vendors in allies' civil networks.[45]

Taking security into consideration now could also prevent significant opportunity costs within collective security architectures like NATO and the EU. So far, there is no single approach to 5G across the nations of these blocs. Anticipating such a 'patchwork quilt' arrangement in Europe and other parts of the world, the US has already stated that it will operate with allies and partners in a 'zero trust' model, and is making the necessary industrial arrangements.[46]

39 BfV (2019), p. 296.
40 Sachverständigenrat - Jahresgutachten des Sachverständigenrates 2016/2017, p. 467.
41 Sachverständigenrat - Jahresgutachten 2016/2017, p. 473.
42 Sachverständigenrat - Jahresgutachten 2019/2020, p. 173.
43 Watts (2019).
44 DoD (2020).
45 FT (2020).
46 DoD (2020).

5 THE OBVIOUS COSTS OF MALICIOUS VENDORS IN 5G NETWORKS

The damage caused by attacks on networks in an attempt to steal or manipulate data is hard to measure. Several sophisticated approaches exist to assess the value of tangible and intangible assets that are destroyed in such an attack.[47] It is, however, easier to estimate the damage of a full-size sabotage of the network. The outage of a network is not exclusive to state-sponsored attacks, but can also happen with criminal intent, by accident or due to natural disasters. The loss of economic activity is therefore well researched. Even when 5G networks do not yet exist or do not yet perform the critical functions previously described, past incidences can serve as an analogy for what a full-size outage could mean for an economy (see, for example, the BlackEnergy malware deployed in 2015 on companies running Ukraine's power grids[48]).

With malicious intention and access to the network, 5G networks can be manipulated. Data speed or latency can be impacted, or the entire network can break down. The obvious costs of malicious – evidentially untrusted – vendors can be illustrated in the following drastic, but less probable, scenario.

In this scenario, assume that a vendor who is untrusted and under the control of a malicious government wishes to integrate a kill switch into European 5G networks. By doing so, this government would possess a tool that would serve as a powerful weapon in political conflict. Of course, this weapon could only be used once because, in the aftermath, the victim or victims would inevitably fully replace the technology. This hypothetical scenario is not unthinkable, given recent events such as the WannaCry ransomware that ripped through companies across the globe, in what was one of the most damaging hacking operations in history.[49]

With regards to China, there already exist several contentious issues that have the potential to damage the country's relationship with western countries, such as the sovereignty of Taiwan, Uygur detention camps, waterways in the South-China Sea, or human rights in Hong-Kong. If a serious international conflict over these or other issues were to arise, it is likely that the possibility of interfering with the supercritical infrastructure of the opponent would become a political option. In the following section, we strive to estimate the economic impact of this. Of course, the political effects of a government being unable to do what it thinks is right because it fears the economic consequences or the loss of sovereignty would be equally disastrous.

Assuming that the underlying technical problem that allowed foreign actors to tamper with European 5G networks would be resolved within days, it would still paralyse most of – or, under pandemic telecommuting circumstances, literally the entire – economy. In order to understand the order of magnitude, it is helpful to think about this on the basis of a numerical example.

Each percentage point of the annual labor days costs about 0.3% of real Gross Domestic Product (GDP) in Germany, according to the German Bundesbank.[50] Its authors specifically had events like holidays and bridge days, as well as adverse weather conditions, in mind: one could extend this to times of general strike. It is a very conservative assumption that an all-embracing work stoppage caused by sabotage would be as costly. In 2019, GDP in Germany amounted to 3.449 billion Euro.[51] Assuming a 20 workdays month (240 workdays a year), one percentage point corresponds to 2.4 workdays. Three days of downtime, for example, due to a kill switch-induced communication blackout would thus correspond to a 0.375% reduction in GDP, which in absolute terms equates to about 12.94 billion Euro. On top of that, there would be cascading effects in the aftermath, including secondary damage, cost of preventive mitigation, rip and replace of fishy hardware and software, and so on.

47 See for example https://www.hermeneut.eu/.
48 Cerulus (2019).
49 Greenberg (2017).
50 Deutsche Bundesbank (2012), p.59, and Hansen und Meyer (2018) p.18.
51 Statistisches Bundesamt (2020).

Applying this estimation approach to two of the three other countries that we cover in our country studies below and in separate dedicated documents – namely, France and Italy – and adding calculations based on figures from the Portuguese Ministry of Finance gives us ballpark figures for these (see Table 5).

Table 5: Estimated costs of a total communication network shutdown

Scenario of total Cost of a Shutdown of X days, in billion €			
	1 day	3 days	6 days
France	2.788	8.363	16.727
Germany	4.313	12.940	25.880
Italy	2.057	6.171	12.342
Portugal	0.425	1.275	2.549

Source: own calculations, based on World Bank[52] data, Bundesbank[53] and Portuguese Ministry of Finance[54].

Not all sectors of the economy would be affected in the same way, and some might prove more resilient and capable of catching up with the foregone production. While it would be near impossible to compensate for unplanned downtime for companies dealing with piecework, the overall effect on the economy depends on its degree of interdependence, with sectors influencing each other and with cascading effects. While short interruptions might be followed by making up leeway, the German federal bank states that such catching up effects cannot be quantified precisely. The Portuguese Ministry of Finance estimates that the costs of a longer interruption, though accumulate disproportionate.[56]

Besides the aforementioned kill switch scenario, which, due to horizontal and vertical segmentation and other precautionary mitigation measures, appears less likely, there is a more feasible but less conversant 'worst case scenario'. Operating, managing and maintaining 5G networks will be highly dependent upon the application of artificial intelligence (for details, refer to section *Artificial Intelligence in 5G Networks* below). The AI algorithms can be tampered with by malicious actors, with severe, yet less visible, consequences.

52 World Bank (2020).
53 Deutsche Bundesbank (2012)
54 Jornaldenegocios (2020)
55 Deutsche Bundesbank (2012)
56 Jornaldenegocios (2020)

6 THE HIDDEN COSTS OF UNTRUSTED VENDORS IN 5G NETWORKS

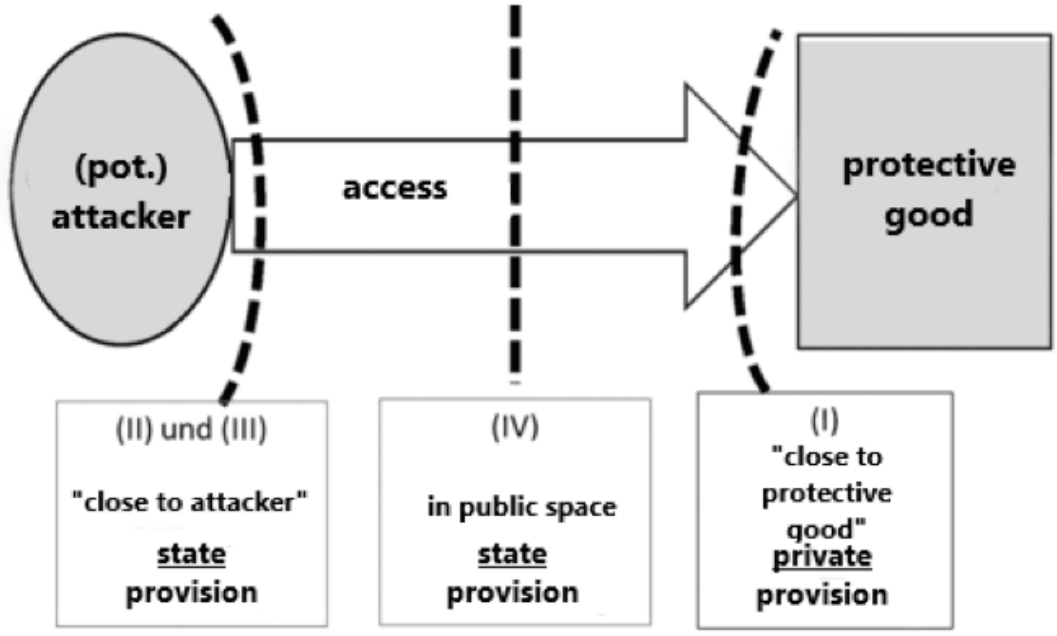
In addition to the obvious costs that incur when a supercritical 5G network is sabotaged, there are also less visible or hidden costs that incur when the confidentiality and integrity of the network and its data is being compromised. These costs are hidden because they occur either later in time or because they are borne by people or institutions other than those who decide upon the architecture (and its parts) of the 5G network. Yet, for society as a whole, these costs are highly relevant and must be considered when deciding whom to trust when building the next generation of network infrastructure.

In the following section, we try to uncover these hidden costs, define them, and in some cases, devise an approach for measuring them. The latter is often difficult or even impossible where we lack the necessary data, but it will nonetheless become clear that it is insufficient to compare the bids of the network vendors for the hard- and software (and sometimes also for the management) to build the network. Instead, the costs for the entire economy over the lifecycle of the network are relevant when making the decision about whom to award the order to build a 5G network.

6.1 The Economic Character of Security

Refusal by the state and mobile network providers to use trusted vendors for the construction of 5G networks shifts the cost of protection towards companies (especially security-sensitive ones) and citizens. According to Bretschneider et.al., it should be the task of the state to intervene preventively close to the perpetrator.[57] Here, protection services take on the character of a public good. The refusal of the state to perform this task shifts the costs and the need for action to the right, towards the owner of the property in need of protection.

Figure 2: State Provision and Private Provision of Security.



Source: based on Bretschneider et. al. (2020), p. 106, translated.

57 Bretschneider et.al. (2020), p. 106 graph 2.

It could also be argued that measures taken to protect the network are also cheaper than having to compensate for this by protecting each and every client connected to that network. Ultimately, it is their data that countries such as China are after. Or, as the German industry association Bitkom puts it: *"…in the economic environment, sabotage, espionage and data theft are aimed at digital data or the information and communication infrastructure of industrial companies. Advanced digitisation makes it increasingly easy for criminals to gain access to this data."* [58]

To put it in more economic terms: **digitalisation is lowering the costs for the attacker** for sabotage and data theft, thereby increasing "profitability" and lowering the barrier to entry for attackers, shifting the supply curve for attacks to the right. Without additional efforts to counter this trend, we will end up in an equilibrium with more successful attacks and higher losses for businesses and citizens. With 5G (and, more importantly, the applications based on it) becoming available, this trend will only increase.

Already SMEs lack sufficient IT- and data security, since the costs for protection are subject to high economies of scale, as well as positive externalities.[59] SMEs also tend to be less digitalised in their value chain. One reason for this is a lack of trust in the security of connecting production to the internet. Consequently, SMEs are less likely to use cloud computing. It is safe to say that this pattern will also be evident when it comes to making use of the opportunities associated with 5G.

Security and digital experts, as well as politicians, repeatedly speak about a **"security by design"** instead of a "functionality first, cybersecurity later" approach. The beginning of a technology implementation is the time to decide against making the same mistake that was made when building the general internet. This mistake entails building a communication network to which we connect crucial parts of our economy, thereby gaining productivity, until the network is abused for criminal or other activities of our adversaries. Only after such damages occur does the protection of an inherently insecure network become important.[60] Of course, **using only trusted vendors** in 5G networks **will not be sufficient** to guarantee a network's security, but it certainly eliminates a significant vector for attacks by our adversaries.

Bitkom claims that already 18% of all cyberattacks on German companies are coming out of China.[61] It does not take much foresight to predict that, **when the attack vector increases** because so many more valuable targets are connected to the network, **so will the number of attacks**. It seems equally as obvious that, if the attack vector is made in China, the share of attacks originating from China will increase.

Security comes at price. The threat of economic and political exploitation by an adversary needs to be compensated for with appropriate protection measures. These measures will require resources, and resources cost money. One intuitive approach to understand this issue is to distinguish between the different types of control. Below, we will differentiate between preventive, reactive and detecting control activities. The underlying idea is that each activity, either in its entirety or in part, must be undertaken because one or more untrusted vendors contribute to the communication network.

Preventive activities are chronologically implemented before any undesirable incident occurs, in order to reduce the threat to the confidentiality, integrity and availability of data. To prevent an attack, resources are used to make it more difficult or costly for the attacker to perform the attack. In the most extreme case, an attack is prevented by not exposing oneself to the risk at all. In our case, this would mean not connecting to a network with untrusted components.

Detecting activities are ongoing, routine-based procedures that allow one to discover anomalies and attacks early on, in order to reduce the scale of the damage. They may include the operation of sensors and Security Operations Centers (SOC), and the screening of lines of code in software patches.

58 Bitkom (2018), p. 16.
59 Park et al. (2008), p. 92.
60 See Herpig (2020), p. 2.
61 See Bitkom (2018), p. 29.

Reactive activities are mitigation measures taken in the aftermath of an attack. Once an attack is detected, the network operator and his affected customers must limit the scale of the damage and ensure that a similar attack cannot happen again. This could also include the replacement of certain technology or software in the network, which could even include a temporary shut-down of the entire service. For the network customers, one option is to shift business away from network operators with untrusted technology, as was observed in the aftermath of the Snowden revelations.

6.2 Prevention and Control

As mentioned earlier, a lack of trust in the confidentiality, integrity and availability of a network requires additional measures in order to secure confidence in the network. These measures can be technological (a solution that allows for the confidentiality, integrity and availability of data in an inherently insecure network) or managerial (various forms of risk management).

Another way to look at such controls – which are basically mitigating measures at different points in time – can be found in the **European Union Toolbox** of risk mitigating measures referring to cybersecurity of 5G networks. It distinguishes between strategic mitigating measures, technical mitigating measures, and supporting actions.[62]

Strategic measures comprise aspects of regulation and supply. Technical measures refer to baseline and specific network security provision, requirements regarding the provision of services and products, resilience, and arrangements enabling continuity in cases of credible contingency. Supporting actions enhance effectivity of measures of both types.

The toolbox has already come into full effect and the European Commission has been working with member states to track the progress of their implementations. While areas of regulatory intervention, for example, are mature enough that they have been reviewed in a positive light, others, such as diversification of supply and technical measures, are still seen as at risk. This speaks to how important it is to design and impose vendor strategies that protect national and European interests, while insuring against the unknown costs of allowing these vendors to be part of a transition to 5G.

The Prague Proposals are of interest here. These were suggested at the Prague 5G Security Conference on May 3, 2019. The proposals are grouped into four categories: policy, technology, economy, and the nexus of security, privacy, and resilience.[63] These proposals, while not binding, have been the backbone of subsequent discussions and commitments undertaken by participating countries as they assess their own individual strategies for auctioning spectrum and transitioning their network security to respond to these demands. The facets of these proposals were amplified and seep into our examinations below.

6.2.1 Technology

Technology to protect the network in the presence of untrusted vendors must guarantee and ensure that existing and new systems set appropriate access control policies, limit access by third parties, and that, when remote access is necessary, zero-trust authentication, authorisation and logging are applied to subsystems so as to ensure there is always visibility on access to data and changes performed. VPN deployment and particularly zero-trust models must be deployed across network infrastructure, management functions and software-defined operations such that access and management is limited to subsystems, that remote access does not imply broad access to equipment and services, and that strict identity is guaranteed for subsystems.

These subsystems must also be appropriately isolated to ensure that access to non-critical systems in this model does not warrant access to any other (more critical subsystems). This means costs increase for every new piece of infrastructure (small cell, edge network infrastructure and associated

62 For more on the EU Toolbox see DG Connect (2020).
63 See Prague Proposals (2019).

software) as not just access must be secured, but also associated firmware, hardware access functions and virtualisation must be secured and standardized, in order to guarantee vendor-specific implementations uphold promises of trust at each stage. **Network Operation Centres (NOC) and Security Operation Centres (SOC) must be run on-premises for MNOs** and in countries where democratic institutions and due process are found.

The vast majority of the operators in a 2017 study (75%) responded that **complexity and cost are blocking the implementation of advanced signaling protection**, and even open specification technology stacks such as OpenSS7, with potentially lower installation and testing costs, see limited adoption due to a focus by commercial entities running the network on the value-adding high-level components of the stack, rather than on its underlying protocols. This risk exposes said high-level components to hidden threats that malicious vendors can exploit.[64]

Furthermore, relying on untrusted vendors will accelerate and widen the adoption of protection solutions and technologies, especially **end-to-end data encryption**. While the direct cost of such a protective measure in terms of infrastructure is decreasing, indirect costs due to increased latency are hard to estimate, as they depend on multiple parameters including the service, the protocol and the encryption schema. As highlighted in the white paper produced by the 5G PPP Security WG *"… End-to-end encryption may hamper the use of multiple value-added security services such as attack detection, QoS monitoring, fine-grained access control, among others …"*. [65] In general terms, the benefits of using encryption have several drawbacks that may be costly when deployed at a large scale.

Even when encryption is ubiquitously introduced, the issue of **metadata security** remains. While the packet payload can be encrypted and thus made unreadable to unauthorised third parties, information about who communicates with whom at which point in time remains in the clear, as networks use this information for routing and accounting purposes. This metadata leakage can be quite revealing: for instance, it would provide detailed insights into the frequency and intensity of business relationships between organisations, be used for stock market manipulation and insider trading, upcoming trade deals, or reveal communication partners of protected occupational groups, to name a few examples. Through its hardware, an untrusted vendor would have access to this metadata information and be able to use it for economic or political advantage.

The abovementioned factors only serve to strengthen the case for end-to-end encryption and zero-trust security architectures that protect end-user data and metadata, as well as secure and isolate access to critical or soft targets of the overall 5G network. Finally, additional security measures must also be taken to safeguard physical access to infrastructure to ensure it performs as deployed and is monitored. However, these physical security measures are independent of the trustworthiness of the vendor.

6.2.2 Cyber threat intelligence

When untrusted technology is an integral part of the network of networks, the latter is confronted with potentially more vulnerabilities and is thereby a greater risk for governments, businesses and citizens. The lower security of such a network can be compensated for at least partially by putting more effort and money into monitoring and controlling the untrusted network. In order to do so, the following is needed:

1. More **oversight** of what is happening in the network,

2. A **testbed** to find out what could happen in and with an untrusted network,

3. An institutional arrangement for **sharing information** among competing network operators and with the national cybersecurity agency.

4. An institutional arrangement to share information within the EU and with like-minded states.

64 ENISA (2018), ITU (2019).
65 5G PPP Security WG.

Foto © gorodenkoff/iStockphoto

A national **Information Sharing and Analysis Center** (ISAC) for 5G networks will be needed regardless, even if the networks only contain trusted technology. Bugs and exploits will always exist. In addition to this, an exchange mechanism through which operators and clients can notify each other about suspicious activities in untrusted networks must be established. While with trusted vendors there is a joint interest in keeping the network safe, with untrusted vendors it is precisely this that is being questioned, and therefore it must be carefully considered if the vendor in this case can be pulled into the circle of trust in which sensitive information is being shared.

The information sharing is pivotal to reduce information costs for each market participant and to ensure that an attack pattern cannot be repeated. However, we know from earlier attempts to share information about cybersecurity incidents in critical infrastructure providers that private companies are reluctant to share such information with competitors or with the government, fearing negative market reactions.

Beyond knowing what is going on in a network, it is also important to know what could be going on. In particular, networks with untrusted technology must be constantly tested for weaknesses or malicious tools that give an attacker access to a network. In an independent 5G test center, a twin of the untrusted network can be tested under lab conditions. White hat hackers can look for loopholes and ways to take control of the network, or covertly distract some of the data.

The **national cybersecurity agency** will have to map the weaknesses of 5G networks and mirror those with the threat information they gain from their own analysis or from partnering intelligence agencies. All these national endeavors will also have to be mirrored at the EU level, for example at ENISA, in order to learn from the experience and knowledge of like-minded countries.

6.2.3 Testbed for 5G networks and applications with untrusted technology

The development of 5G networks is not yet finished. Future upgrades will enable the networks to perform more functions and thereby enable new business models. For the improvement of 5G networks, and for the development of applications, much research and development still needs to be

done. For this reason, R&D laboratories and testbeds are a necessary infrastructure.

Such labs and testbeds are also needed to learn more about the vulnerabilities of networks and, in particular, of those which include untrusted technology. During the test conducted to help the UK government determine if Chinese technology can be part of future 5G networks in Britain, it became evident just how many resources are needed for this endeavor. Consequently, the UK's National Cyber Security Centre recommended the establishment of a **National Telecoms Lab** that could test networks under various conditions and with a variation of vendor technologies.[66]

To calculate the costs of such a test center, with a top-down approach, one can look for analogies that already exist. A recent example is the Fraunhofer Institute for Integrated Circuits, which was awarded a testbed as part of the 5G Bavaria initiative. As initial funding, they received a grant from the State Ministry of Commerce of more than EUR 25 million.[67] In order to run such a specialised, applied research institute, more funds are necessary.

The staff required to test and control in a satisfactory manner the security of the telecommunication devices implemented in France can be estimated at a minimum of 150 multidisciplinary experts. High-level engineers and lawyers, working together in order to check also the commercial contracts, verify if technical translations provided by suppliers of foreign origin are sincere and faithful to reality, and prepare legal texts. The total desirable payroll therefore tends towards an approximate and minimal range of EUR 12-16 million per year, to which operating costs must also be added. According to the expansive technical means due to be allocated for such a mission (laboratory, test beds, etc.), the total budget in the case of untrusted telecommunication suppliers may be estimated at EUR 30 million per year.

Of course, research institutes come in different sizes, depending on the scope of the issues on which they are working. Coming from such research institutes ourselves, we find it realistic and necessary that a national institute fully devoted to 5G network security is needed to test and verify the software from untrusted vendors over the lifetime of a 5G network. A feasible benchmark which confirms these orders of magnitude: the IRT-SystemX research center, focused on digital security needs analysis concerning IoT, communicating vehicles and industry 4.0, has been dimensioned with a staff of 140 people – mainly researchers – and a budget of EUR 23 million per year. Depending on the size of the economy, the amount will of course vary.

An alternative bottom-up approach to calculate the costs of testing and verifying the trustworthiness of a software and the network is by estimating the costs of a source code review. White box testing of a product based on a source code review is a common method for products with a strong link to security, and a variety of vendors offer governments and independent auditors the option to evaluate their products' source code as a trust-building measure. A significant and common example of this is Microsoft's Government Security Program.[68] In the following section, we will estimate the potential costs of such a source code review in the case of 5G.

Simply put, the auditing cost is a function of the product magnitude, the rate at which it can be audited, and the associated costs for the audit process itself, as well as organisational overhead. The functionality of a product is provided by both software and hardware, which require different auditing approaches, where the complexity of the former is typically measured in metrics such as source lines of code or SLOC. The costs of a software code audit can therefore be approximated by:

product SLOC * avg. SLOC review capability/hour * auditor cost/hour.

This provides an upper bound to the costs of a software review, as not all parts of a software are equally as important with respect to security. Consider the case of an operating system, which includes, for example, functionality to display contents on the screen, to receive user input from the

66 NCSC (2020), p. 25.
67 Fraunhofer IIS (2020).
68 For more information see https://www.microsoft.com/en-us/securityengineering/gsp.

mouse and keyboard, to communicate over the network, and to manage user and file permissions. If a vendor has malicious intent to take control over devices sold to customers, some places, such as the software code for user management or file permissions, would serve as prime targets for such a backdoor, while others would only provide limited utility for an adversary. The same reasoning also holds true for 5G, which includes a lot of functionality, for instance for managing the wireless interface or signal processing. For a more practical estimate of auditing costs, the above calculation would hence be discounted by the portion of the product with direct security implications, which might range between 15% and 30%, depending on the type of component.

There are several data points to approximate the software complexity of 5G Radio Access Network components. The latest release of the vendor-neutral, open-source implementation OpenRAN from June 2020 contains a total of 1,089,389 SLOC, while the commercial vendor Ericsson stated that "the software complexity of [their] RAN in a baseband exceeds that of Boeing 787 aircraft."[69], which would set a lower bound at 6.5 million SLOC.[70] Additional expenditures would need to be budgeted for the review of embedded system firmware, chipset's microcode[71] and the verification of hardware designs.

The scientific literature on **source code review** efficiency is sparse. However, a study by a vendor of software engineering toolkits found that code review performance of up to 500 SLOC per hour is attainable in practice, beyond which the efficiency in detecting errors significantly declines.[72]

For a calculation of use, we would assume an average salary for a security-trained software engineer of EUR 125,000 per year, and apply the standard 25% overhead procedure followed by European Union grants. Based on 1600 working hours per year, the upper bound for a software audit of the OpenRAN implementation could be estimated at EUR 212,500 while the equivalent commercial product from Ericsson would tally at EUR 1.25 million for a source code review. The number might be discounted, as discussed above, if only select portions of the code would need to be inspected.

There are, however, additional aspects that may need to be considered. As a new technology and largely software-based product, it can be expected that vendors will put out new product features and issue bug fixes as well as **software updates in regular succession** after the initial product deployment. Thus, the source code audit would need to be continuously repeated in order to assert the security of future modifications. Although such modifications might occur regularly, the bulk of the product would remain unchanged, which also means that the bulk of the auditing expenses are upfront, whereas updates can be evaluated at a fraction of the initial price tag.

Auditing the product's source code is, however, only part of the procedure to ensure a secure 5G deployment. The audit procedures need to be highly integrated into the product rollout to ensure that the reviewed source code is actually the same software that is shipped to the units installed in the field. This requires arrangements with the product manufacturer and additional processes at the customer stage to **control and audit the supply chain**, which creates further costs.

Additionally, the presence of untrusted vendors means that an incentive for added end-to-end **data flow monitoring** exists beyond that present in a secure-by-design network architecture. Mechanisms for monitoring and logging need to be implemented, with additional associated retention and secure storage policies and devices. Moreover, vendors also need to preempt the existence of bad actors and perform various checks of data and metadata integrity and security, communication channel security and data handling processes and devices, including end-user and IoT devices. Security across all domains must then be ensured so that services and data sent, stored, and processed within the 5G system must be stored, preserved

69 Ericsson (2020c).
70 Information is beautiful (2020).
71 Chips, processor and memory hardware can be manipulated to receive remote commands from foreign entities, through different backdoors: higher layer software services may be strictly scrutinised but rely on lower layers which are not necessarily.
72 Smartbear (2019).

and its integrity guaranteed. Horizontal security will also guarantee that data sent over the system is always confidentially and integrity protected. This means that extraordinary security measures must be demanded at the device and gateway level, the network and access level, the data and applicational level (particularly important due to the increased importance of software in 5G), and the physical access level. Vendors are trying to incorporate these concerns into their network design (which introduces performance and cost tradeoffs)[73] by staffing up and building resilience in their security offerings in order to then offer these capabilities to MNOs[74] and use them internally as well as to guarantee new revenue[75].

6.2.4 Artificial Intelligence in 5G Networks

Artificial Intelligence (AI) has emerged as a viable and effective solution in several application domains and is an enabler for the deployment of 5G networks. Specific care has been taken so that the MNOs are aware of the security risks associated with 5G. As 5G is an emerging technology, an evaluation of the costs to avoid or mitigate these risks is not possible. Therefore, in contrast to the rest of this policy paper, the next subsections have primarily the aim of creating awareness of potentially (hidden) costs of adopting an untrusted vendor.

Motivations for AI in 5G networks and related costs

AI is the simulation of human intelligence processes by machines. AI programs focus on three primary cognitive skills:

- **learning**, also called training (acquiring data and creating rules for sorting that data),
- **reasoning** (choosing the right data to achieve the desired outcome), and
- **self-correction** (fine-tuning the data and sorting for the most accurate results).

For such skills, the larger the input of data, the better the results. 5G networks generate the enormous amounts of data that AI needs to operate. At the same time, AI can be instrumental in managing the complexity of and helping to protect 5G networks.

According to a report by Ericsson "What role will Artificial Intelligence have in the mobile networks of the future?"[76], AI is increasingly adopted into mobile networks by MNOs. Applications of AI, already implemented by MNOs, are, among others, intelligent anomaly detection and prediction, planning of network capacity, and smart filtering of the network alarms.

To further highlight the potential, but also the challenges of AI, the goal for MNOs and decision-makers in general is to build a so-called "zero-touch" network. These networks will be characterised by no longer requiring human intervention other than high-level declarative and implementations.[77] The system measures and understands the context and regulates the network. Though extraordinarily beneficial and cost-effective, this entails a loss of controllability and the need for novel methods and indicators to measure the actual reliability (security) and performance of the overall AI system.

Risk analysis and cost evaluation

At the basis of AI employment is the training process, critical to providing accurate and reliable results. The training (and refinement) is an ongoing process that leverages the vast amount of data generated by the 5G network devices. Quality of the training data is therefore crucial for the AI's controlling actions. If there is a fault or bias in the input data, the impact affects operation and business services of the CSP. In the case of intentional manipulation, training data can be altered on purpose to force an AI to commit the wrong actions, with severe consequences in terms of costs, efficiency, and security.

It is not trivial to identify and quantify the hidden

73 https://www.rcrwireless.com/20160623/internet-of-things/energy-versus-security-iot-security-tradeoff-tag28
74 https://www.nokia.com/about-us/news/releases/2019/10/31/nokia-launches-netguard-adaptive-security-operations-for-5g-era/
75 https://www.ericsson.com/en/blog/2020/10/how-to-master-e2e-network-security-when-introducing-5g-core
76 Ericsson (2019).
77 Ekudden (2018), p. 3.

costs associated with the adoption of AI in 5G when deploying equipment from untrusted vendors. One possible approach is to interact and gather information, in qualitative and quantitative terms, directly from MNOs. Indeed, cost models or analytics of general validity to exploit for evaluation purposes are not available in academic literature. AI is an emerging technology, and the focus of current R&D works are mainly on exploring its benefits, assuming a fully controlled and secure 5G network environment.

A multi-dimensional evaluation needs to be brought about, as

- economic (e.g. loss of revenue for diminished subscriptions),
- social (e.g. innovation hurdles),
- technical (e.g. efficiency loss, low service quality) and
- political (e.g. loss of confidence and trust, difficulties in achieving compliance to regulations)

issues are all relevant. As several dimensions of cost are concerned with the AI technology (and its applications), in the following section, the goal is to clarify the types of hidden costs. Hereafter, the focus is on the manipulation of the AI system, as the hidden cost associated with the cloning of the AI core model(s) can be very high.

Evolutionary roadmaps of interviewed MNOs position a full adoption of AI-based network controllers in the second wave of 5G implementation. Consequently, most will reconsider the threats posed at that stage. However, since AIs will be based on the data collected from the network devices that are currently installed, today's decisions on how to build the network have an impact on the future level of trust into AI managed networks.

There are three types of cost for an out-of-order AI system (i.e. malfunctioning because of a data or model poisoning):

1. Cost of issue detection

2. Cost of created damage

3. Cost of fixing the issue (e.g. rip and replace)

Cost of detection

For these costs, the crucial point is to carry out (at least periodically) an impact analysis to verify that the AI system is working properly. For this purpose, data collection, analysis and validation (for streams or pools of data) need to be executed. Costs of this type decrease alongside the growth of trust and reliability in the AI performance.

Cost of damage

This type of cost exists in several domains: economic, social, technical and political. Examples might be (i) loss of market share (e.g. for subscribers' churn due to low service quality), (ii) loss of credibility or opportunity (e.g. for unreliable services or service support system), (iii) loss of competitive advantage (e.g. for inadequate offers or lower efficiency), (iv) bad network planning or Operation & Maintenance, (v) penalty or fine for missed fulfilment of SLAs or regulations compliance.

Cost of fixing

These types of costs are somehow similar to other security costs: fixing anomalies is a complex operation, especially for potentially pervasive AIs. These costs are identical to mitigation or permanent fixing of a security risk. However, in this case, a rip and replace is unlikely without a long downtime window: (re)training the AI system takes time and resources. This specific cost is therefore among those with the highest impact.

Contacted MNOs share confidence that AI systems adopted for core services (e.g. anomaly detection and automatic trouble ticket generation) are safe enough to operate in a secure environment. They share concerns about AIs when used for management and orchestration of network. One consideration comes from a recent Nokia report[78] which suggests a 5G deployment architecture that adds threat remediations at the application layer. The proposed

78 Nokia (2020).

architecture, according to the EU 5G toolbox, assumes an underlying heterogeneous technological layer (i.e. different technological providers).

6.2.5 Regulatory costs

The potential supply of untrusted vendors for the 5G infrastructure requires additional efforts and expenses for security regulations of network equipment in the political and legislative process, as well as for network operators using this equipment. Network operators bear the risk of a violation of certain regulations by reason of negligence. Stakeholders who are responsible for framing the legislation must define additional parameters that ensure a secure network environment while guaranteeing a level playing field. Even with an untrusted vendor being part of a 5G infrastructure, the legislative framework and regulation must strive for sufficient security of users, by requiring additional protection measures from MNOs or users through appropriate regulation.


Foto © gremlin/iStockphoto

Before a regulation or a law is passed, many entities take part in the consultative, legislative and implementation process. Stakeholders and decision-makers are ministries and parliamentary committees who oversee the interdisciplinary topic alongside competent authorities, industry associations, standardisation, and audit institutions, as well as network operators. In contrast to a market where technical infrastructure is only deployed by trusted vendors, potential threats due to untrusted vendors must be explored legally and measures to avoid possible security breaches must be analysed in more depth within the legislative process.

Given that, political institutions and authorities will face increased efforts because of more complex decision-making processes (e.g. interdepartmental coordination) and higher personal expenditures based on the sheer quantity and quality of regulative specifications and the purchase of external technical and legal expertise before passing a relevant law. Therefore, the costs of regulation are not exclusively a burden for the stakeholders that must comply with it (or face the risk of sanctioning, for example e.g. fines if they fail to do so). Incrementally, the funder of the regulator (mostly the taxpayer) incurs costs accumulating due to the regulating process itself. This applies to the equipped network as well as to all regulation of connected systems.

Once passed, a more complex regulation, which is particularly necessary when an untrusted vendor is part of the 5G infrastructure, implies more costs for any market participant who operates under this regulation as well as for the audit authorities. The presence of an untrusted vendor increases the demand for the provision of technical expertise in an audit authority, and leads to higher administrative expenses due to the more complex regulation and the frequency and intensity of auditing. In order to meet this demand, audit authorities' costs rise either by employing more and highly educated and scarce personnel, or the commission of certified external services, who are able and available to perform the audit (e.g. the German Federal Office for Information Security has certified eight providers according to Common Criteria for Information Technology Security Evaluation CC[79]). Besides the certification, the need for more frequent audits will only be met if service providers have enough capacities to perform this ministration. A lack of trained or available personnel on the provider's site will lead to delays to the auditing processes and higher costs for the authorities.

79 BSI (2020).

Market participants such as network operators are required to comply with the regulations. In order to fulfil more complex regulations, companies will presumably be confronted with additional expenditures due to training and communication, the development of equally complex and strict certification for their suppliers, and the risk of legal actions following infringements. Additionally, those more specific and wider regulations must be transferred to the company comprehensively. This may require thematically enlarged liaison offices, support from legal counselors, workshops for, for example, the procurement personnel, and continuous exchange with the competent authorities and decision-makers.[80]

Regulatory cost as part of the hidden costs of untrusted vendors can only be defined and calculated if the law, as well as additional efforts and expenses, are solely determined as a consequence of or counter-measure due to untrusted vendors. While the general presence of untrusted vendors requires more detailed regulations, and increased efforts to implement and comply with those, it cannot be quantified precisely which of the additional expenses arise solely as a result of the presence of untrusted vendors.

Certifications for, for example, particular IT-security levels of equipment will nonetheless apply to avoid malicious attackers, irrespective of the vendors' trustworthiness. Nevertheless, the illustration of the outcome of selected regulations gives an impression of the budgetary scope of regulatory costs regarding IT security. Find below in Table 6 estimations of topic-related regulations for Germany, provided by the German National Regulatory Control Council (Nationaler Normenkontrollrat).

Table 6: Expected annual compliance cost of selected regulations (German examples)

Cost bearer	*Required Expenses (extracts)*	*Expected amount in €*
	IT Security Act 2015[81]	
Administration	Staff (425 additional posts) at BSI (220), BKA (80), BfV (50), other authorities (75), material costs	38,000,000
Economy	Reporting security incidents	9,000,000
		47,000,000
		+ 6,000,000 (non-recurring)
	Implementation of EU Directive 2016/1148 in Germany (NIS Directive)[82]	
Administration	Staff (181,5 additional post), mainly at the BSI	14,300,000
Economy	Reporting security incidents	13,200,000
		27,500,000
	IT Security Act 2.0 (expected 2021)[83]	
Administration	Staff (948 additional posts) at BSI (799), BKA (90), BNetzA (34), BDBOS (21), BMI (4), material costs	125,800,000
Economy	Reporting security incidents	9,000,000
		134,800,000
		+ 28,800,000 (non-recurring)

80 Voland and Büsch (2020).
81 Normenkontrollrat (2014).
82 Normenkontrollrat (2016).
83 BMI (2020).

6.2.6 Insurance

Cyber insurance is **a risk management tool**. A company transfers the cyber risk into the hands of an insurer for a price. The price is dependent on the size of the risk and is smaller if the company is taking action for its cyber protection.

Already 14% of companies in **Germany** have bought cyber insurance, including 32% of all larger firms.[84] In **France**, where the total amount of insurance premium was EUR 80 million in 2018, the market is rapidly growing, but still very small in comparison with the US. This figure conceals large disparities: following costly attacks against Saint Gobain and Renault, about 100% of France's big and publicly traded companies now take out cyber insurance. On the other end of the spectrum, only a few per cent of the SMEs and very small enterprises (which represent more that 99% of French companies) take out cyber insurance.[85]

Damages caused by attacks on 5G networks must be borne by someone: either by the network operator or by their customers. If the MNO is liable for the damage, a common way to deal with this risk is to buy insurance. However the insurance policy will typically demand that the MNO meets certain security standards in order for the insurance to cover the damage. The insurer could therefore become a quasi-regulator of the 5G equipment market. Since these types of new risk are difficult to calculate because of a lack of past data, insurers will limit their risk exposure to well-defined damages and limit the coverage. These limits are quickly reached when business interruption is covered by the policy.

From 2017 to 2019, IRT SystemX conducted a study to investigate the management of cyber risk throughout the value chain and its transferability to insurance.[86][87] The study highlighted "the lack of prior experience about previous cyber incidents" facing insurance companies. The study also shed light on the aggravating factor of silent covers, or non-affirmative covers. Compared to other risk categories, insurance companies have fewer than 10 years of cyber incidents records. This brief history does not cover all types of incidents, and even fewer have as yet resulted in losses. The existing history mainly corresponds to ransomware, malware and phishing incidents while many other categories exist. Additionally, any new technology – and 5G is the perfect example – bears new types of risks.

However, in 5G networks, the **evaluation of insurance compensation capacity is more complex** and problematic, especially in the presence of untrusted vendors. Insurance companies covering the risk of infringements in such contexts will likely call for higher or even **prohibitively high premiums** for their offers in communication environments using untrusted vendors, or assess the **risk to be uncoverable** from an insurer's perspective. For society, this could mean that the state must jump in as the **insurer of last resort**, as they had to with nuclear energy. Several European governments had to provide guarantees for nuclear power plants run by private utility companies since the new 'nuclear' risk was considered uncoverable by insurers. A similarly complex situation could arise when insurers invoke a war risk clause when a foreign government is suspected of being behind an attack.

At present, insurers do not have all the actuarial elements they need to size their insurance offering for 5G networks, particularly regarding intangible data, which is not yet subject to legal qualification or financial and accounting quantification. Without a reliable risk analysis method and an exhaustive cyber incidents history, the boundaries of such risk will remain unclear and its consequences on a global scale seem uncontrollable. In such a context, insurers and reinsurers will probably adapt their policies when their customers start connecting their production to 5G networks. Strict liability limits in the insurance policies seem likely. It will be interesting to see, then, if insurers will play a prescriber role in the choice of telecom operator, especially for security sensitive actors and companies with higher threat level in terms of intellectual property and data privacy.

84 Bitkom (2018), p. 51.
85 Commission ad hoc Cyber Risk (2018).
86 Cotelle et al. (2015).
87 Cotelle et al. (2019).

Foto © Ildo Frazao/iStockphoto

6.3 Shift of Demand

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 ensure 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, in particular, **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 providers**, would take the same precautionary measures. Just think of the German electricity grid provider 50Hertz in which a Chinese company wanted to buy 20% of the stakes. That deal was ultimately prevented by the German government for security reasons, as they feared that China could take control of vital German utilities.[88]

There are various definitions of critical infrastructures, and the composition of sectors differ even among EU member countries. The following sectors are usually referred to:

- energy,
- information technology,
- telecommunications,
- transport,
- health,
- water,
- food,
- finance and insurance.

These sectors are not reflected in national accounting one-to-one. For example, in the case of Germany it is still possible to derive approximated values for at least some of them by adding together public services, health, education (18.8%), financial and insurance service providers (3.9%), information and communication (4.6%), totaling

88 BMWi (2018).

27.3%.[89] Assuming that this proportion is reflected in the structure of business customers of the telecommunication sector – a quarter of those belonging to critical infrastructures – we derive that up to 27% of the turnover of the communication sector (public sector and corporate customers) might shift towards MNOs with only trusted vendors. These customers can then 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, at least in security sensitive applications.

While the first shift – customers switching operators – is rather a business-management consideration for the operators when making decisions about their choice of vendors, it nonetheless falls into the category of hidden costs. Not connecting to 5G networks and the associated foregone productivity gains bear an external cost of the MNO's decision from whom to procure the network technology.

The size of the possible shift in demand of critical infrastructure providers (see table 7 below) could be calculated as follows:

$$D_t^{mtl\ cr} = R_t^{tl} * S_t^{mts} * Sh_t^{bc} * GDP_t^{cr}$$

with

$D_t^{mtl\ cr}$ = demand of critical infrastructure industries for mobile telecommunication services

R_t^{tl} = revenue of telecommunication services in time period year t

S_t^{mts} = share of mobile telecommunication services of total services in time period year t

Sh_t^{bc} = share of business customers of all customers in time period year t

GDP_t^{cr} = relative contribution of critical infrastructure industries to GDP in time period year t

t = time period, year of consideration

Table 7: Potential shift of demand of critical infrastructure industries away from MNOs operating untrusted networks

Critical Infrastructure Industries	Shift of Demand
Germany	2,496,501,000 €
France[90]	474,880,000 €
Italy	929,235,000 €
Portugal[91]	97,238,000 €

Source: own estimations.

89 Statistisches Bundesamt (2020). The definition of critical infrastructure in Germany (organizations or institutions of major importance to the state community, the failure or impairment of which would result in sustained supply shortages, significant disruption to public safety or other dramatic consequences) is based on economic sectors. Please note that the sector of Education is tabulated by the German Federal Statistical Office in one category with Public Services, and Health, and cannot be computationally eliminated here.

90 The figure for France seems surprisingly low compared with that for Germany, but on the one hand the revenue of telecommunications service providers in France as a whole was only just over half as large, and on the other hand the proportion of business customers in Germany is almost twice as large. Furthermore, the contribution of the CRITIS companies to the gross domestic product in France is lower in percentage terms than in Germany.

91 The low number is due to a very narrow definition of what is considered a critical infrastructure in Portugal.

Another shift, or lack of shift, concerns the location choices of security-sensitive companies from abroad. These will make their choice of location dependent not least on the existence of a secure communications network in the countries being considered for their foreign direct investment (FDI).[92]

Other security-sensitive customers include the security and defence sector, R&D intensive industries, or other industries with special security and safety risks. R&D intensive activities are particularly vulnerable to corporate or state-run espionage and infringement of intellectual property. Relevant sectors include pharmacy, electronics, nanotechnology, and more. As an example, just look at the many current espionage attempts around the coronavirus vaccine development.[93]

The global trade of digital goods and services is gaining importance domestically and in international trade. Big data exploitation comes with significant potential of revenue growth of 2.9 per cent and up to 3.6 per cent cost reduction per year.[94] Annual GDP in Europe could increase by up to EUR 1.9 trillion by 2025 if data analytics and IoT are implemented and used.[95] Not participating in this trend towards more digital trade out of risk aversion means incurring high opportunity costs and falling behind the competition.

All industries that depend on the availability and integrity of their data streams to do business will want to secure them. Industries with distinct safety requirements must be insulated from manipulation and resulting risks to human life and physical integrity, including space, aviation, automobile, robotics, and others. Connecting to a 5G network with untrusted components is something they will consider twice.

A possible approach to quantifying the impact of such a pre-contract loss is to analyse data of government spending for telecommunication services. This data should be available in government budgets. One might multiply this by the number of comparable security-sensitive government bodies and estimate the potential overall lost revenue for MNOs. With a more top-down approach, one can assume that the **IPR-intensive industry** equals the security sensitive industry. Around 45% of the total economic activity (GDP) in the EU is attributable to IPR-intensive industries, worth EUR 6.6 trillion.[96] If one further assumes that the costs of telecommunications services are distributed in the same way as their share of GDP, 45% of turnover with business customers could be willing to shift their business to an MNO with only trusted vendors or will shy away from 5G entirely.

The size of the possible shift of IPR-intensive customers (see table 8) could be calculated as follows:

$$D_t^{mtl\ ipr} = R_t^{tl} * S_t^{mts} * Sh_t^{bc} * GDP_t^{ipr}$$

with

$D_t^{mtl\ ipr}$ = demand of IPR intensive industries for mobile telecommunication services

R_t^{tl} = revenue of telecommunication services in time period year t

S_t^{mts} = share of mobile telecommunication services of total services in time period year t

Sh_t^{bc} = share of business customers of all customers in time period year t

GDP_t^{ipr} = relative contribution of IPR intensive industries to GDP in time period year t

t = time period, year of consideration

92 Security in various dimensions has been established as a statistically highly significant determinant of FDI, for instance by Busse and Hefeker (2007) with regard to "government stability, internal and external conflict, corruption, ethnic tensions, law and order, democratic accountability of government, and quality of bureaucracy" (Hammami et al., 2020).
93 Williams (2020).
94 Brookings Institution (2017).
95 Bughin et al. (2016).
96 EUIPO (2019).

Table 8: Potential shift of demand of intellectual property rights intensive industries away from MNOs operating untrusted networks

IPR-intensive Industries	Shift of Demand
Germany[97]	4,613,904,000 €
France	1,009,120,000 €
Italy	1,259,570,000 €
Portugal	344,386,000 €

Source: own estimations.

We are aware that there is an overlap between the IPR-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 MNO's sales with corporate customers are in question here, and should have a tendency to migrate towards trusted networks.

For KRITIS, it is also foreseeable that using only trusted networks might be required through regulation in the future, and for other businesses, cyber insurance companies could make it a requirement for their customers or their vendors who want to be part of a value chain (i.e the automobile industry). In addition, since the benefits of 5G are primarily in business applications, we predict the MNO's business volume with corporate customers to relatively increase.

This potential shift of demand of corporate customers should be seen in perspective with the current cost claims of MNOs regarding rip and replace. Using only trusted vendors for 5G networks could help to keep and even gain sales with corporate clients.

Redundant Infrastructure

If governments refrain from using privately operated networks with untrusted technology, they will consider running their own network for their communication needs. Since we are examining the economic impact for society as a whole rather than the business consequences for individual or all companies in the telecommunications sector, the interesting questions boils down to: how much more expensive would it be for the society if the government made a make-or-buy decision in favor of a state-run network? Based on the assumption that a statal communications provider, which in some countries must first be founded, is less efficient than a private one, the economic burden of such an inefficient second-best solution would be the difference in full-cost pricing between the statal and the private network.

An example of how costly a security-motivated setup of a redundant statal communication infrastructure is the Netz des Bundes (Federal Network) in Germany. In the planning phase, it was assumed that (besides the initial costs of transition into regular operation of EUR 100 million by federal institutions) the annual fulfillment costs of around EUR 92.2 million from the operation of the federal network would be far below the costs of around EUR 160 million per year that would arise from external operation of the federal network.[98] The project later ran out of the rudder in terms of finance and delays. Because the project Netz des Bundes was delayed by six years and had increased its costs from EUR 114 to 426 million[99], the Ministry of Finance has blocked expenditures for the project in 2020.[100] In other words, installing the infrastructure came with additional sunk costs amounting to EUR 312 million. Most of this was rooted in rented but unused data centers, procurement of expensive hardware that was not used, and costs for poorly supervised external IT consultants.

97 The reason for the costs of Germany being so much higher compared to Italy and France is the higher IPR-intensity of the economy and a much larger share of business customers in the market for mobile services.
98 Federal Council (2016).
99 German Federal Court of Auditors (2017).
100 Federal Law Gazette (2020).

6.4 Change of supply

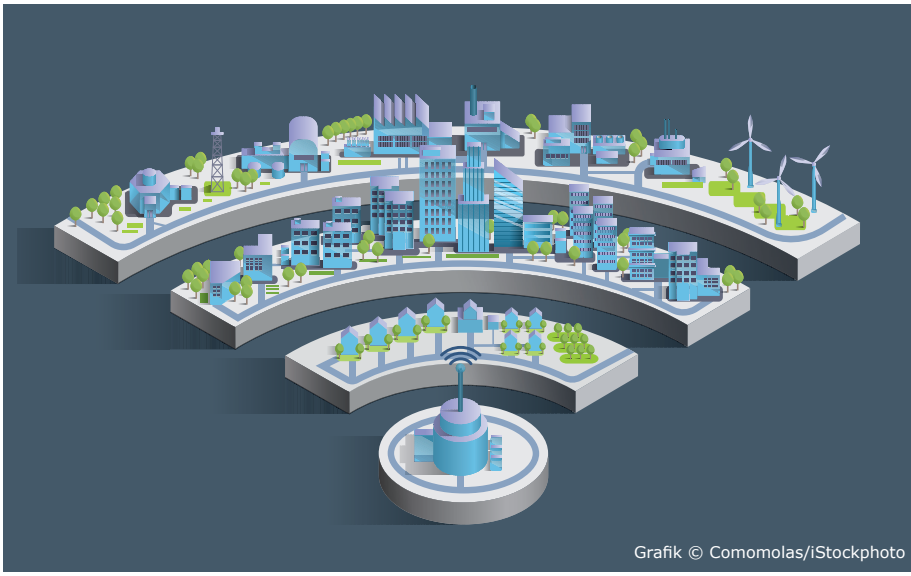
Chinese producers of 5G technology are currently facing **export restrictions** imposed by the US government on inputs designed and produced with US technologies (for example semiconductors).[101] These restrictions significantly affect Chinese vendors' capabilities to produce 5G components. They also raise doubts about the quality that can be delivered if it lacks the first-best supplier's components. If the solution is to replace US technology, such as micro-chips, with Chinese technology, this will even further deteriorate the trust in such network components in the West.

Japanese and South Korean chips are potential **second-best substitutes**, unless similar restrictions are passed on them. For instance, companies supplying products to China's most important chipmaker, Semiconductor Manufacturing International Corporation (SMIC), were recently notified by the US Department of Commerce that continuing to do so constituted an "unacceptable risk" of such products being diverted to "military end use"[102], and were discouraged from keeping their business ties.

Another aspect relating to supplier competition concerns vendor (proprietary, customer) **lock-in effects**. Among the possible causes of lock-ins are unfair pricing practices. European and South Korean competitors are accusing Huawei of selling products below cost price.[103] This **dumping** can be meaningful for a profit-oriented working business enterprise only as a short to medium-term strategic measure to force competitors out of the market. It is only possible in the absence of sanctions by competition authorities and with sufficient financial staying power or hidden subsidies from the home state.

The hidden costs of sourcing products from a supplier that forces its competitors out of the market through dumping typically only become apparent after time. If the remaining western suppliers of network technology leave the business, Europe would be fully dependent on Chinese technology for critical infrastructure and for handling our data. This is of particular importance when looking beyond 5G and into the future towards 6G.

As experienced previously by other industries, once competitors from the West exit the market, prices rise again. However, (re-)entering the market is difficult and much effort and equity is needed. The economic rent of mobile network production would likely end up wholly in China.



Grafik © Comomolas/iStockphoto

The lack of competitive pressure, in combination with the by then already proven willingness to abuse their market power, will result in structural financial disadvantages for MNOs and ultimately for consumers, where higher costs lead to higher prices. In a second-round effect, the remaining vendor(s) will have an incentive to raise prices above the cost price, because of:

a. Motivation: the dumping phase was costly to the vendor (unless this was compensated by the home state), and

b. Opportunity: price elasticity of demand is higher than in a competitive market, as MNOs have little choice left as to which vendor to procure.

101 Globaltrademag.com (2020).
102 Financial Times (2020a).
103 Washington Post (2019) and Strand Consult (2019).

Another lock-in related question links to foregone gains in bargaining power and their downstream effects. With global procurement of MNOs, and the roll-out of OpenRAN on the horizon, the market power should shift towards the operators. However, this economic benefit resulting from continuous, or at least periodically recurring, competition does not apply if a network supplier does not participate in openRAN.

6.4.1 OpenRAN and its Impact on Supply

Restricting the choices of MNOs with regards to the array of potential suppliers of 5G communication network equipment has been met with reservations from competition guardians about a too-high degree of market concentration on the supply side. These objections may, however, be short-sighted, given recent market developments and innovations.

In the previous mobile communication network generations, including 4G, vendor proprietary hardware components were incompatible with those of competitor vendors. This made switching to another vendor a very costly decision for MNOs. Even after a MNO settled for a vendor or group of vendors at the core, they did not have the ability to scale radio networks at the user access level easily, based on demand, with multi-vendor procurement. One vendor offering RAN deployments with proprietary technology at low prices meant others would be locked out of competing in large swathes of the access network, unless the buyer (often a MNO) replaced most of it in a single swoop.

OpenRAN changes this market dynamic and has already. MNOs who choose to use OpenRAN will be able to pick their hardware from a much larger group of vendors instead of being forced to use specific vendor-customised products. MNOs will be able to use **commercial off-the-shelf** (COTS) components, as products from different producers can be used on the same network level and even on the same site. This will open up the possibility for **Neutral Hosting** and other types of infrastructure sharing that lower the cost of deployments and allow new use cases to emerge that foster the growth of consumer services and small businesses. Market power of established vendors will decline significantly, in favour of competition and consumer welfare, and many new types of secure, standards-based networks will emerge.

Both Chinese vendors so far have not been characterised by a communicated willingness to participate in the OpenRAN initiative. Instead, they are focusing on lobbying against it due to its alleged performance, scalability and operational complexity concerns. They continue to push for their own proprietary hardware and connectivity standards in their 5G offerings, which will, in turn, make a transition towards an open connectivity market much harder in the future.

These alleged concerns have not materialised in early deployments, with Vodafone running OpenRAN-based 4G and 5G trials in the UK and elsewhere. Rakuten is notoriously executing large-scale multi-vendor deployments in Japan using OpenRAN. In fact, Rakuten says its network "has been built 40% cheaper than would have been possible using traditional vendors and which is running at 30% below the expected operating costs of running a traditional mobile network".[104] This has inspired European partners such as Telefonica to sign an MoU with them to push the development and deployment of OpenRAN-based 5G infrastructure.

European and Korean vendors are also taking a more open and proactive stance and have been actively contributing to the evolution and rapid deployment of networks based on OpenRAN standards. Hidden costs of procuring from untrusted vendors in this context therefore relate to foregone flexibility, competition and consumer welfare. It is also possible that OpenRAN will significantly reduce the **first-mover-advantage**, since it is only soon becoming widely available.

6.4.2 Market structure

Another point concerning competition on 5G network markets relates to the overall market structure. The telecom equipment market in most western European countries can be characterised by an oligopoly-oligopsony structure. Academic literature

104 Le Maistre (2020).

on bargaining and competition still suggests for a market characterised by high technology and innovation intensity an efficient outcome.[105] One can therefore assess that the potential cutback of an exclusion of untrusted vendors on competition remains negligible.

Furthermore, as telecom network equipment vendors report relatively large gross margins on sales, they also have a lot to lose in the case of reductions of sales quantities. If one applies tools of critical loss analysis and calculates that vendors would lose around 13 per cent of their sales in that case, they increase prices by mere five per cent.[106] As buyers – that is, the MNOs – are quite concentrated in most European countries, and all-or-nothing offers are a typical bargaining tactic in such circumstances, little danger of price increases is anticipated after an exclusion decision.

On the vendor side, the two Chinese vendors have a market share of 48 per cent in the 4G RAN equipment market in all of Europe. In three countries, 4G RAN is entirely equipped by Huawei and ZTE (for example Belgium, Cyprus and Denmark's Faroe Islands). In 15 countries, their market share is above 50 per cent (for example Germany, Greece and Italy).[107]

Delays in roll-out of 5G network equipment seem not to have materialised in countries that made decisions or passed laws *de jure* or *de facto* excluding untrusted vendors altogether from participation. Screened quarterly and annual reports filed to the United States Securities and Exchange Commission make no mention of delays or increased purchase costs.[108]

These findings are concordant with our findings from interviews with western vendors. One example is the rollout of a 5G network furnished by Ericsson in Denmark within ten months, despite Corona pandemic constraints. One of the Danish telecom groups, TDC, decided in the spring of 2019 against purchasing from Huawei for security reasons. Fears that this decision would lead to significant delays in the roll-out of 5G not only did not materialise, but the ultimately selected European provider managed to complete the roll-out three months faster than originally planned[109], despite pandemic conditions in 2020. That is not to say that there are no delays in the roll-out of 5G. However, these are mostly due to political or legal issues (for example between established 4G MNOs and potential market entrees).

105 For example Baldwin & Krugman (1988).
106 Wagener (2020).
107 Strand Consult (2020).
108 Strand Consult (2020).
109 Ericsson (2020b).

6.5 Productivity Costs

The hidden costs of relying on untrusted vendors also revolve around foregone productivity gains, stagnation or even losses in productivity – in other words, **opportunity costs**. The underlying causes relate to the incomplete exploitation of the potential of 5G due to users' security concerns.

These concerns already exist in many companies, for example concerning cloud computing or connecting the production process to the internet at all. Risk aversion and security concerns can easily lead to loss of productivity. In particular, micro, small and medium sized enterprises that do not have their own IT security department and network security resources, and lack inhouse encryption competence, tend to continue or regain the tendency to localise data instead of exploiting the possibilities of cloud-based processes and products. This precludes the utilisation of seamless and low-friction collaborative tools, and thus hampers the efficiency of use of the workforce and time, as well as of resources. Redundant and obsolescent technology will also have to be maintained. To make this more tangible, it's about the mechatronics company with its own server in the basement and without cloud backup.

According to a study by Bitkom Research in which 553 companies were surveyed, 73 per cent utilized cloud computing in 2018.[110] However, 73 per cent of non-users are concerned about the security of their data and worry about unauthorised access to sensitive company data; 64 per cent are concerned about a potential loss of data; and another 51 per cent suspect an ambiguous legal situation. If security concerns leave some market participants doubting whether the use of digital innovative technology will expose them or their data to an unmanageable risk of data theft and espionage, potential growth is foregone. These foregone potential productivity gains end up as being the costs of a lack of trust in mobile networks with untrusted technology.

The global debate about Chinese technology in 5G networks and the fact that already significant Allied countries have decided to prevent or phase out such technology from their networks will certainly influence decision-makers at the company level on whether to make use of 5G applications in their businesses.

Another point to highlight is the hidden costs created by interoperability and security issues. As mentioned earlier, the necessity for including more security technology in untrusted 5G networks in order to (partially) compensate for the lack of trust in the used technology will slow down the speed of the network. This is particularly worth bearing in mind given that the gain in speed is a part of the productivity gain moving from 4G to 5G. Not getting the full potential or speed out of 5G, then, are costs directly connected with the level of trust in the used technology.

Another point closely connected with the additional security measures is the rise of complexity in project management. Having to worry about and coordinate the various technological and managerial security aspects takes time and energy from company management and creates costs. Management may feel they must decide between losing a company's competitive advantage due to too much risk exposure by having to connect the crown jewels to an untrusted network, and losing the advantage because competitors catch up through digitalization that it itself is shying away from. Again, the described challenge is not unique to 5G or untrusted vendors, but to increases in scale of the lack of trust in the new networks.

110 KPMG (2019).

7 COSTS FOR AFTER-INCIDENT REACTION

In the case it transpires that policymakers and MNOs were mistaken in trusting the vendor of 5G technology and the certainty grows that the vendor colluded with an adversary to violate the confidentiality, integrity or availability of data or a network, a political, organisational and technical reaction must follow. All three are costly. Sanctions, embargoes or military action come at a price that a society must be willing to pay or sacrifice its sovereignty. None of these political costs we wish to elaborate on in this context.

The first step of every reaction must be a thorough investigation into the attack strategy, and should include determining attribution of the attack, the attacker's master, and who gains from the attack (7.1). A second step is a damage assessment that requires additional scarce resources. The third step is to prevent a similar event from recurring (7.2). In this instance, time has a major impact on costs. Once trust is violated, the untrusted vendor becomes a malicious vendor that, ultimately, can no longer be part of a critical infrastructure (7.3). But does it mean that the infrastructure must immediately no longer be used until the untrusted supplier is replaced? Or can the network be operated until the technology is being phased out at the end of its depreciation period?

7.1 Investigation and Attribution

Investigating occurrences such as cyberattacks is recognised as a complex discipline. 5G networks pose new and important challenges to traditional forensics approaches. For instance, the unique identifiers that link to smartphones and connected devices in current telecom networks will be replaced by temporary certificates that are renewed by each antenna. Furthermore, standard forensics techniques and guidelines, such as ISO/IEC 27037:2012 or NIST SP 800-101, are more likely to fail to cope with the highly complex and dynamic nature of 5G networks.

The default investigation workflow[111] is less effective and practical when the evidence left by attacks and/or attackers are spread across different and fragmented domains and locations, with potentially different and conflicting regulation, complicating evidence collection and processing. Monitoring tools lack proper solutions targeted for forensics analysis when the data to be collected and processed involve hundreds or thousands of devices. Classical Security Information and Event Management (SIEM) solutions are not adapted to process 5G data and have limited capabilities to support ex post distribution of liability.

Digital investigation of 5G networks needs to be cross-disciplinary and actively involve law enforcement authorities to guarantee secure access, collection and delivery of cyberattacks evidence. Such collaboration requires a high degree of trust between the different stakeholders. In the presence of untrusted equipment, the tools and the evidence provided by the equipment manufacturer might weaken the results and findings of the investigation.

7.2 Damage Assessment

The generally erroneous assessment of the damage of an incident stems from the nature and the sensitivity of the information that companies are obliged to reveal, namely the theft of personal data, bank details or medical information. As a result, the calculation of the costs of an attack is usually limited to the tip of the iceberg and only takes into account those related to customer information, credit monitoring, legal disputes and regulatory sanctions.

111 Preparation, data identification, data preservation, data examination, investigation and report.

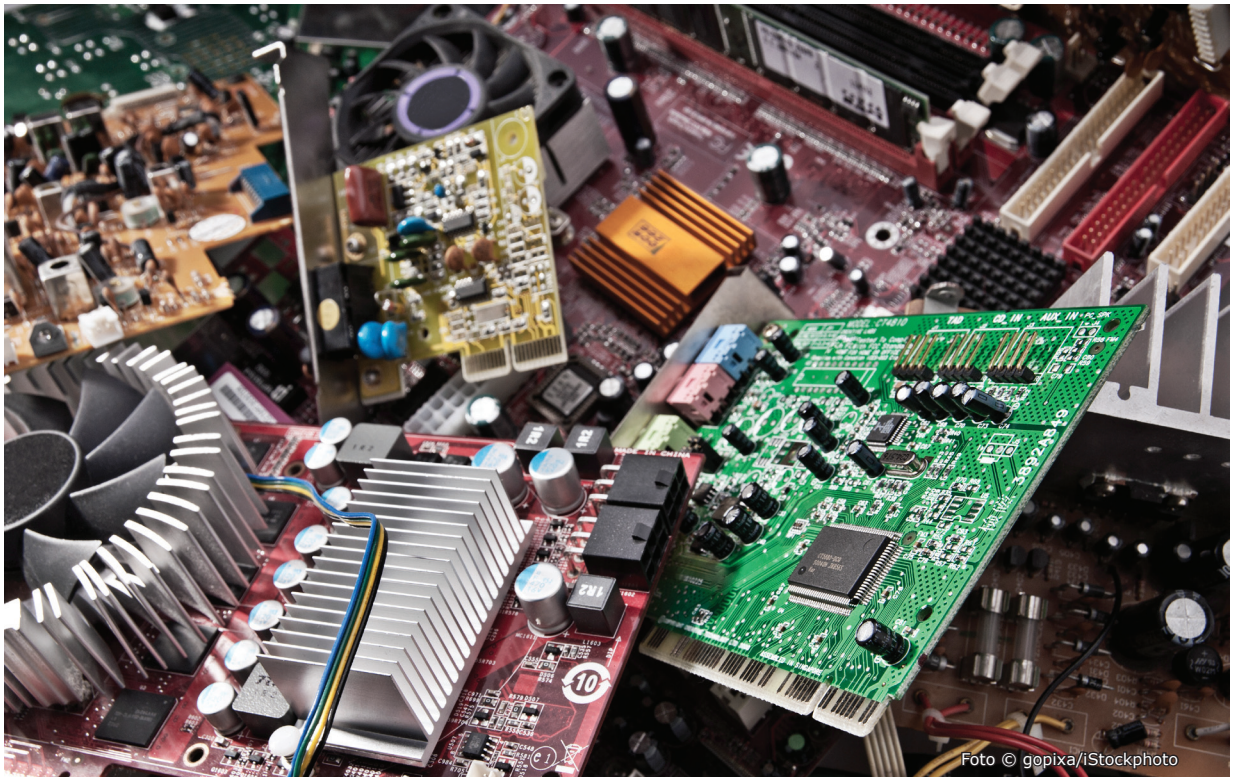


Foto © gopixa/iStockphoto

5G will most likely make such assessment more complicated, as a single attack can have multiple cascading and propagating impacts, leading to objectives other than simply stealing data. In such cases, the impacts can be more far-reaching, and the costs can be particularly difficult to assess. Just think of the recent (2019) ransomware attacks on more than 23 local governments in Texas.[112] Such attacks render citywide smart services unavailable to citizens, creating significant damage to local businesses.

Existing damage assessment frameworks, such as the ones proposed in ISO standards (27000 or 21434), define damage as *"adverse consequence or undesirable result due to the compromise of cybersecurity property (or properties) of an asset, or of a group of assets".* Thus, the damage only refers to the feared scenario that security measures aim to prevent or mitigate. The quantification of the damage is generally performed by using the impact rating that aims at estimating the magnitude of damage due to the compromise of one of the security properties. As 5G spans both digital and physical worlds, we believe that impact needs to be assessed with respect to four core categories: **Safety, Financial, Operational and Privacy**, as defined in ISO 26262.

Safety and security are two distinct concepts that are regularly tied up with one another. The most critical application area where safety risks have an impact today is in the context of Cyber-Physical Systems (CPS),[113] such as those used in Digital Manufacturing (Industry 4.0) or Intelligent Transport Systems. Most critical CPS systems typically implement Safety Instrumented Systems (SIS), which are designed to execute control functions to maintain safe operation and ensure minimal human or environmental damage. However, if connected to 5G, such systems could be made inoperative by a malicious actor, causing severe accidents.

Furthermore, industry 5.0 will be characterised by the cooperation between machines and human beings, with the ultimate aim to give added value to

112 According to NIST, „Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas. Cyber-physical systems will bring advances in personalized health care, emergency response, traffic flow management." https://www.nist.gov/el/cyber-physical-systems.

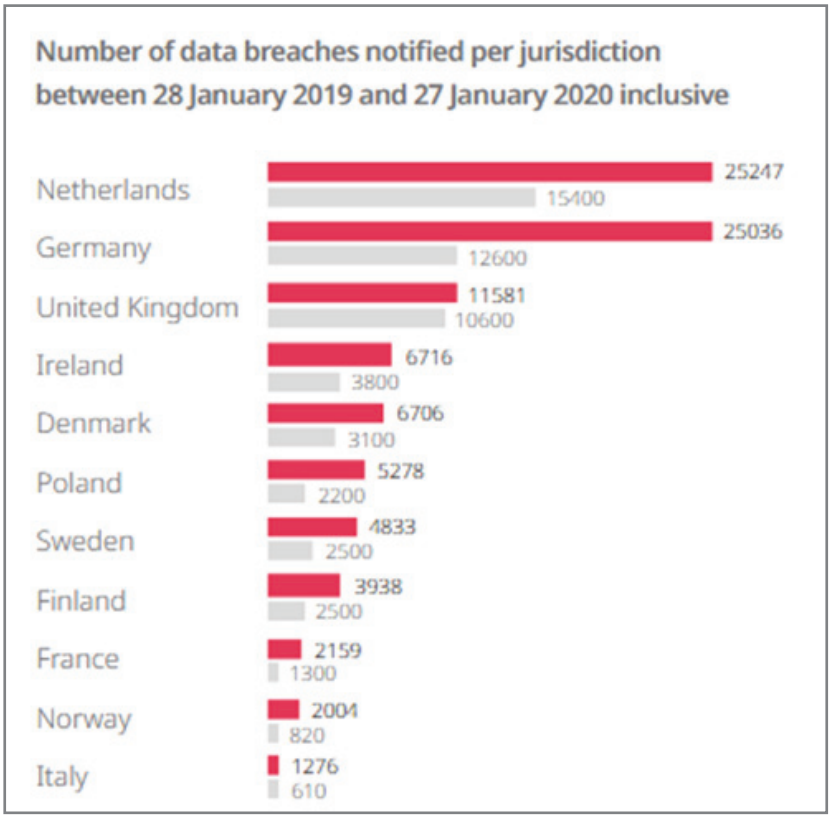
113 See Bischoff (2020).

production by creating personalised products able to meet customers' requirements. The collaboration of humans with advanced machines, for example, collaborative robots, constitutes new challenges for process safety. The ISO 10218 is the most relevant standards series wherein safety requirements for collaborative robots are defined. However, threats that might emerge from untrusted 5G equipment are challenging the effectiveness and practicality of these standards.

The **financial** damage of incidents can include costs occurring in various fields. Legal expenses, liabilities and fines arising from loss of sensitive customer data, loss of sales revenue due to competitors counterfeiting products, additional working expenses due to change management and workarounds, and ad hoc acquisition of backup and side track information technology, are just some of the cost items straining affected companies. The financial damage rooted in data breaches is difficult to assess. IBM published a report[114] on this subject in November 2020. Based on this report, we assess the costs that can be attributed to untrusted vendors in 5G in the respective country studies.

IBM, in the report mentioned above, calculate the average damage of a data breach per country. In Figure 3 we show the number of notified breaches per country in 2019. The huge difference between countries is noticeable, that is due to different national regulation concerning mandatory reporting. The unrealistically low numbers for France and Italy limit the informative value for these countries and demands additional assumptions.

Figure 3



Source: DLA Piper (2020).

114 IBM (2020).

The attack vector of a breach can be manifold. We therefore consider the share of data in transit through 5G networks and the share of untrusted technology in these networks.[115] Ultimately the formula for the costs of data breaches because of untrusted vendors in 5G networks looks like this:

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

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

If the attacks are attributed to untrusted vendors the taxpayer will have to bear the costs of the then-inevitable process of adaptation of regulation. In the case of a post-incident reactive rip and replace (more on this below in Section 7.3), the cost would be far higher than that of a preventive phase-out. While the latter can be planned, controlled, and managed by the MNO in close coordination with the trusted vendors, the former will come as a surprise and a known unknown. Undoubtedly a sudden rip and replace will become significantly more costly, since a new vendor with access capacity has to be available.

Clearly the extent of the additional cost will vary with the size of the project. While a smaller network (in a smaller country) might be squeezed into the plans of a network vendor, a large additional contract will stretch the capacity to its limits. The necessary availability of qualified personnel seems to us to be the biggest cost driver in this scenario.

On an **operational** level, it seems that we are already flooded with hyper-connected devices generating massive data flow. 5G will further accelerate this connectivity. This significant increase in the number of connected devices will irrevocably result in a growth and acceleration of cyberattacks using 5G networks. For instance, in Industry 5.0, data are generated at the "edge" by Industrial Internet of Things (IIoT) sensors distributed on the production floor of a factory and passed along a relatively complex chain of "handlers".

115 The three phases of the data life cycle are (1) ingestion (acquisition from local sensors), (2) data in transit and (3) data at rest. Lord (2019).

In such a complex and multi-tier context, trust in the data and the transportation network are the key factors. A potentially untrusted network layer means, in general terms, a loss of trust in the entire industrial control system. Private networks are not subjected to the EU Toolbox and can be installed without legal limitations, nor are they subject to golden power requirements. In addition to this, in the industrial business, rip and replace costs are often unaffordable, because they mostly require disruption of the service and breaks in productivity.

Privacy refers to the damage that occurs after the exposure or the leakage of digital information conveying private information. Different entities are affected by this category of damage, ranging from the company that leaked the data to the end-user and customer that is concerned by the exposed data. The first category (i.e. company or organisation) will automatically fall under the existing general-purpose regulatory frameworks. When data pertaining to European citizens is concerned, GDPR establishes fines of up to 4% of annual revenues or EUR 20 million, whichever is higher. Companies such as British Airways (EUR 204.6 million), H&M (EUR 35.3 million), Google (approx. EUR 50 million) or TIM (approx. EUR 27.8 million), the Italian telecommunications operator, have already been issued or have actually paid fines issued by their respective data protection authorities.

In addition to the aforementioned fines, the societal and indirect economic risks, via reputational damages, are too large to ignore, with studies surfacing that companies exposed to a data breach typically underperform on the NASDAQ by an average 3.7% after only a year.[116] Victims (65%) report loss of trust in an organisation and 85% report that they are likely to inform others of their negative experiences. [117]

7.3 Rip and Replace

A major argument of those who oppose a ban of untrusted vendors in 5G networks are the associated costs that undoubtedly occur when untrusted technology that is already installed has to be removed, causing sunk costs, and when old contracts need to be cancelled and new ones negotiated. For example, Deutsche Telekom claims that if they were not allowed to use Huawei as a vendor for their 5G network and had to replace Huawei's existing technology from their 4G network, the overall cost would be EUR 3 billion.[118] These costs will first fall on the MNOs, but will also be passed on (at least in parts) to their customers.

Procurement from trusted vendors would also mean that prices no longer include the earlier described "discount" untrusted vendors offer their customers. The external costs associated with the untrustworthiness that were borne by 5G customers would now fall on the MNOs. However, these costs ultimately can and will be passed on to customers.

Ultimately, the rip-and-replace-argument by MNOs is a bet on China not exploiting the opportunities that arise with gaining access to western 5G networks through politically controlled companies over the lifespan of the untrusted technology. Alternatively, if China does exploit these, it is a bet on the exploitation at least remaining unrecognised.

In case MNOs lose this bet and the "smoking gun" is found by the authorities, cyber experts, or by customers themselves, the reputational damage for MNOs will be enormous. Alerted customers will switch providers and it is highly likely that regulators will demand a speedy replacement of the (no longer untrusted, but now evidently) malicious technology. If this scenario is found to be realistic, it is only a matter of when, and not if, the costs for rip and replace will occur. And, clearly, the costs of replacing untrusted technology later in the life cycle of 5G will be more expensive than doing it sooner while 3G / UMTS is still functioning and investments into improving 4G networks still take place.

116 Ponemon Institute (2017).
117 Winder (2019).
118 Handelsblatt (2020).

If this scenario doesn't seem likely, it may be useful to look at already uncovered and well-researched cases, such as that of the African Union (AU) or Papua New Guinea (PNG).

In the former, China built and equipped the new headquarters of the AU in Addis Ababa as a gift to the multinational organisation. This gift included an IT network with technology from Huawei and, to a lesser degree, ZTE. It later transpired that, every night, the network transferred large data packages to a network in China without the AU's knowledge or intention. In the aftermath, the AU replaced the entire IT equipment of the AU, and only trustworthy suppliers and service providers were eligible to participate in it.[119]

In the latter case, China loaned PNG, through the Exim bank, USD 53 million in order to have Huawei build a data centre in PNG's capital Port Moresby, as part of the Integrated Government Information System (IGIS). Exim Bank is mandated with "implementing Beijing's trade and strategic objectives".[120] The center became operational just in time for the Asia-Pacific Cooperation (APEC) leaders' meeting. The newly built data center had numerous serious – and in all probability, deliberate – inbuilt security flaws.[121] These were discovered only by chance when PNG sought financial assistance from Australia to remedy shortcomings in conservation measures. China also funded more digital infrastructure in PNG, including the biometric identity card and the national broadband network.[122]

Another case that sheds an unflattering light on the trustworthiness of a major Chinese supplier can be found in recent reports about the discriminatory targeting of ethnic minorities by facial recognition software, "likely to cause further distrust of the company in the West"[123] [124].

119 Sherman (2019).
120 The Australian Financial Review (2020).
121 The Australian Financial Review (2020).
122 ASPI (2020).
123 Endgadget (2020).
124 Washington Post (2020).

8 CONCLUSION AND SCENARIOS

It is difficult to estimate the economic costs of untrusted vendors in 5G communication networks in Europe with any degree of accuracy. One reason for this is that the future significance of this new technology for the economy and society can only be estimated, and many questions remain open-ended. Another reason is that external costs are borne by market participants other than the MNOs. A third reason is the temporal distribution of the costs. A holistic estimation approach would therefore be based on shaky ground from the outset. What is possible, however, is the recording of minimum orders of magnitude in some areas – thus an **additive estimation approach** that seeks to make visible an expected minimum for various reasons of currently hidden costs.

This additive approach will vary from country to country in terms of its content – the components that can be estimated – and in terms of its outcome, which will also depend on the size of the respective economy and its composition. For this reason, we will turn to individual countries in the context of country studies. These country studies will hopefully help put decision-makers on strategic course for setting the regulation of an infrastructure and technology of almost incalculable importance for at least a decade.

In an **appendix** to this policy paper following this chapter, we summarise the result of these country studies. In case one is interested in a particular country, we recommend reading the full country study that is available as a separate document.

The various cost categories we have discussed above clearly demonstrate that a society cannot leave to the MNOs alone to choose the supplier for the future supercritical infrastructure. While buying products for a dumping price might be beneficial from an individual business perspective (but beware of the lock-in effect), it certainly is not for the economy as a whole.

The promise of **OpenRAN** with a more open 5G network architecture, which will allow MNOs to choose from a larger spectrum of vendors and which would also allow them to more easily substitute single components of their network, will **shift market power** towards the operators. MNOs should therefore consider this alternative approach to building a network and should weigh up for themselves whether it is worth the possible delay until OpenRAN becomes operational on a large scale.

However, the economic effect of **delay in 5G availability** is sometimes exaggerated. Since the "killer applications" for 5G still need to be developed, and so do many of the 5G compatible devices, the new network generation is "just" a much faster mobile network for faster internet access. The big gains in productivity will materialise only later in time.

While many of the measures discussed will have to be implemented independently of the choice of the vendor, the level of **trust in the vendor** as a company, but also the regulatory framework within which a company operates, does make a significant difference in the scale of costs. If trust comes into doubt, the **rule of law** becomes the next best substitute for trust. In this respect, the five system vendors differ immensely. To say the least, experience shows that suing a company in China for malpractice and compensation has less probability of success than in countries with high rule of law.

Decision-makers should reach a decision from several available and sometimes mutually exclusive alternatives that take all political, technical, economic and societal aspects into account. These decisions are associated with uncertainties, as the accuracy of the assumptions could be questioned in a fast-moving environment. In this **dynamic environment**, having or gaining **flexibility is of great value** for all market participants (maybe with the exception of the vendors).

One method to support decision-making in situations of high complexity and uncertainty is **scenario building**. The scenario technique originates from the field of economics and has the advantage of allowing three concrete alternatives to be calculated or simulated. With this technique, as-

sumptions on individual values can be adjusted in a systematic way and the effects can subsequently be checked. As a result, uncertainties with respect to the decision-making process can be significantly reduced and the respective options can be reviewed. The most basic form of scenario building provides three scenarios: optimistic (which we call here goldilocks), pessimistic (which we call Armageddon) and realistic.

8.1 Goldilocks Scenario

China is keeping its promises. Huawei and ZTE will not be asked to inappropriately collude with the Chinese Communist Party (CCP). While they could be forced to do so by law, the CCP is more interested in the long-term business success of Huawei and ZTE and will not endanger this by using the access they could get to Western 5G networks through them. Unlike with all traditional cyber tools that are being used by China's intelligence community and related hacker groups, the opportunities arising from 5G will not be used (see section *Productivity Costs* above, specifically on opportunity costs). Unlike with past experience in various industries, China feels like it is already competitive enough in fields such as Industry 4.0 and the things that are going on in western factories and R&D centres. It will not use the possibilities 5G offers to learn about the chip industry, which it so desperately tries to copy at the moment (see sections *Regulatory Costs, Insurance, Shift of Demand, Change of Supply*). Unlike with COVID vaccine development, China will not exploit the possibilities that arise from 5G-controlled laboratories and experiments.

The EU and its member states can ignore the dependence on 5G technology from China when deciding on the status of Taiwan in international organisations, when considering sanctions on China over violations of international law, maritime law, and human rights. Lock-in effects cannot be exploited by the Chinese vendors because, with the widespread adoption of OpenRAN, the market power has shifted in favor of the MNOs. It is therefore a waste of money and resources if MNOs do not take the cheapest offer of vendors that help them build the networks.

Basic security costs will have to be implemented anyway to secure networks from cyber criminals and third-country espionage. The foreign policy strategy known in German as "*Wandel durch Handel*", or political change through economic exchange, will finally succeed and China, in the next decade, will become a country with stronger rule of law and respect for property rights.

We find this scenario very optimistic and believe that hope is not a strategy. Instead, one can hope for the best, but should prepare for the worst.

8.2 Armageddon Scenario

MNOs choose the cheapest vendor to build their 5G networks. Huawei and ZTE together gain a large market share in western Europe for 5G technology. The networks work properly and reliably, therefore a large part of the economy manages their value chain over these 5G networks. Finally, governments, with their various entities, make use of the manifold opportunities digitalisation has to offer. So does the military and other security organisations. Because of deeper European integration, security and intelligence institutions strengthen their cooperation and interoperability, in particular when it comes to new capabilities, the latter often relying on 5G technology.

While China continues to expand its economy and global international influence, it continuously fails to honor basic human rights domestically as well as in countries and territories under its influence. It also does not respect international law or the law of the seas. The EU will stand up for its values and use its economic and political strength to pressure China to comply with these international norms with economic sanctions, granting an increasing


Foto © CribbVisuals/iStockphoto

number of political activists from China asylum, and European Navies participate in freedom of navigation maneuvers.

At this point, the CCP decides it wants to teach the Europeans a lesson. All of a sudden, the networks in Europe go crazy. They stop working properly and businesses experience cascading effects from the 5G networks into other critical infrastructures. Because public and most of private transportation comes to a standstill, hospitals return to a paper and pencil management, which greatly reduces their capacity. The European economies tank. At worst, all this is happening parallel to another political crisis or a pandemic.

To build workarounds that do not rely on 5G technology takes weeks, but for productivity to go back to pre-crisis levels a reboot of 5G networks – this time without Chinese technology – is necessary and takes further time. While dealing with the domestic crisis, the EU and member states have no appetite for further international conflict. China will use the situation to further increase its international influence. The costs to society will therefore be huge, as described in Chapter 5, and similar to those we currently experience due to pandemic-induced shutdowns. Furthermore, there is no longer any argument about what would have been the economically rational choice when choosing a vendor for 5G networks.

We find this scenario to be unlikely, but possible. We come to this conclusion because such a large-scale 5G shut down is almost like the nuclear option for the cyberworld. And, as we know from history, countries are, luckily, reluctant to make use of such a devastating option. But the analogy is also somewhat misleading. Unlike kinetic weapons, such a cyber tool has only one shot. Once fired and attributed, countries will get rid of the technology that acted as the port of entry into their networks, thereby making it impossible to use it again. Consequently, such action would also have a severe impact on the future business opportunities of the aggressor country. The aggressor in this scenario also cannot be certain that the attack will remain unanswered, and if is answered, it may not be limited to the cyber world.

8.3 Realistic Scenario

The realistic scenario starts out like the Armageddon scenario. In this case, however, China does not make use of its potential option to almost completely shut down the European economies. Instead, it uses covert access to the supercritical infrastructure to gain knowledge and insights about European businesses, research institutions, governments and political actors. It does so to the point that there remains some credible deniability to remain under the threshold for the countries to retaliate in a meaningful way and to rip and replace the suspicious technology.

The knowledge gained through these operations will help China and some Chinese businesses to further gain political and market power globally. National and EU attempts to catch up (or to keep its competitive advantage) with the US and China technologically will be less effective since intellectual property cannot be properly protected. Ericsson and Nokia will lose its currently still strong market position and will play no role in 6G in the twenty-thirties. Sweden and Finland will by then be frustrated, blaming Germany and France and claiming that, if it had been for example Siemens and Alcatel, these EU power houses would not have allowed this to have happened.

Some security-sensitive companies will replace Huawei and ZTE 5G technology in their private networks and maybe switch to an OpenRAN system in which they only allow trusted vendors. Alternatively, they cut off 5G for those parts of the company that they consider the crown jewels of their value chain. The European intelligence community will come out of this stronger, since they turned out to be right when predicting: *The global political situation and China's related political and economic ambitions lead us to expect a further intensification of espionage and influence activities*.[125] The military and security apparatus will build their own network with European RAN technology. Yet, since among the EU states eavesdropping is not unheard of, there will also be a push for a more national-centered approach, undermining the unity of the EU.

The costs in such a scenario will remain mostly hidden and will contain all the elements we discussed in Chapter 6. These costs are clearly higher than what can be gained from the lower costs of untrusted vendors, and once this becomes more visible to policymakers and the public, compensatory measures will be taken. Ultimately, it is foreseeable in this scenario that countries and MNOs will end up replacing untrusted technology at some point. One could summarise by saying that, after all that, they pay twice for this new technology.

We find this to be the most likely scenario, given what we know and have learned over the course of this study, and under the assumption of *ceteris paribus*. This is, of course, unless western European governments decide on regulation that effectively restricts Chinese access to 5G networks. We are aware that such a decision will have second-round effects, such as retaliation from China, that need to be taken into account by policymakers.

As we finish this study, we see some initiative by the EU Commission to move in this direction. Asking member states to *"(a)ssess the risk profile of suppliers; as a consequence,* ***apply relevant restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks - for key assets*** *defined as critical and sensitive in the EU coordinated risk assessment (e.g. core network functions, network management and orchestration functions, and access network functions)".*[126] The report rightly points out that *"(p)rogress is urgently needed to mitigate the risk of dependency on high-risk suppliers, also with a view to reducing dependencies at Union level."*[127] Many member states have taken or plan measures to limit the risk coming from untrusted vendors and thereby compensate for the external costs their usage imposes on European societies. However, questions remain whether these measure, if adopted, will be sufficient.

We wholeheartedly support the Commission's actions to strengthen research for 6G development as part of the Horizon Europe research framework

125 BfV (2019), p. 298.
126 EU Commission (2020), p.7, emphasis by the authors.
127 EU Commission (2020), p. 9.

programme.[128] However, we believe that a dedicated test center for 5G security is needed and would be a worthwhile EU endeavor. We hope that by uncovering the hidden costs of untrusted vendors in 5G networks we have contributed to the debate of the research community, but also and more importantly to the political debate about how to properly regulate the building and operation of the next generation critical infrastructure.

128 EU Commission (2020), p. 12f.

9 APPENDIX: SYNTHESIS OF COUNTRY STUDIES FOR FRANCE, GERMANY, ITALY AND PORTUGAL

9.1 Introduction

In the chapters above, we examined what the costs of untrustworthy technology in 5G networks are and how they can be determined, if necessary. On this basis, we have prepared a number of country studies for France, Germany, Italy and Portugal and calculated individual cost categories. In this appendix, we briefly summarise these country studies and present the key results.

The costs described here are only a sub-set of costs that untrusted vendors could drive in to the financial, economic and political 'balance sheets' of MNOs, customers and taxpayers, as the mapping table of cost categories shown in the executive summary makes clear.

National economies, telecoms markets and regulatory progress naturally have a great influence on costs, so this chapter firstly describes briefly the 5G landscape and regulatory context in each country.

9.2 The 5G landscape in Germany, France, Italy and Portugal

9.2.1 Germany

German stakeholders run a moderate risk of incurring hidden costs from untrusted 5G vendors if the draft for an IT-Security Law 2.0 comes into effect and is fully executed. Otherwise substantial risk for German industry exists.

Development of 5G networks in Germany is in the hands of largely familiar mobile network operators, but will incorporate a different vendor mix from 3G and 4G networks. There are three existing MNOs: Vodafone, Telefonica Deutschland, and Deutsche Telekom. A new, fourth MNO, 1&1 (Drillisch), will evolve its role from a leaser of others' network bandwidth to become a dedicated operator. Though the existing MNOs all have untrusted vendor hardware in their 4G infrastructure, none of the four companies seem to plan to use Chinese 5G vendors in their future 5G core networks anymore. Vodafone and Deutsche Telekom may use Huawei in their Radio Access Networks, while 1&1 plans an OpenRAN roll-out.

The German government has had strategy for 5G outlined since 2016, with a goal of becoming a leading market for 5G applications. In parallel with policy, since 2015 the parliament has developed effective legislation to ensure Germany's IT security needs. The Second IT Security Act (IT-SiG 2.0), at the end of 2020 in the draft stage, introduces a double-test procedure for Chinese systems. This requires vendors to self-declare their trustworthiness, which must also be attested by five ministries and security agencies. This stringent regime is regarded to most likely exclude untrusted vendors from German networks in the future.

Development of this legislation reflects near universal scepticism of Chinese vendors, with most political parties advocating positions encompassing laws to ensure trustworthiness to outright exclusion. However, the governing CDU/CSU is internally split over the issue, which complicated the decision-making process within the government.

9.2.2 France

French stakeholders run a low risk of incurring hidden costs from untrusted 5G vendors.

In France, there are four MNOs leading the introduction of 5G infrastructures – Orange, SFR, Bouygues and FREE. Orange has the greatest market share at present. In September 2020, these companies purchased licenses for spectrum to offer 5G services for the next 15 years. Each MNO is required to set up 10,500 antennae by 2025 to support the French government's goals of a fully completed 5G network by 2030. 5G rollout started in November 2020, with the turning on of an antenna in Nice, and is expected to be completed city by city. In the near future, rollout will focus only on the 5G RAN. The core network will remain on 4G technology at first. Only two of four suppliers use Huawei's 4G equipment; Huawei has only a 20% share of the French 4G equipment market, and its share of the 5G equipment is expected to be at a lower level (in the range of 15 to 20%).

Concerns about untrusted vendors have been voiced across civil society, the government, and the political spectrum. The French telecoms market is already well-regulated; three institutions[129] play a key role balancing ambitious government rollout plans with cyber security and competition concerns. Additional articles were adopted into the French Post and Electronic Communications code in 2019 and 2020, to ensure security concerns were managed. Now, MNOs are required to submit applications to the French Cybersecurity Agency (ANSSI). Of 157 applications to date, all 75 'reduced duration authorisations' and rejected applications concerning Chinese equipment. The French state is currently under legal challenge for requiring Bouygues to have removed 3,000 Huawei antennae and base stations in urban areas by 2028.

9.2.3 Italy

Italian stakeholders can still run a low-to-moderate risk of incurring hidden costs from untrusted 5G vendors.

The three main Italian MNOs – TIM, Vodafone and WINDTRE – have begun introducing 5G services to business and consumer customers in the major Italian cities. Two smaller MNOs, Iliad and Fastweb, are aiming to launch services early in 2021. Italy is one of a majority of EU countries with a 4G infrastructure where greater than 50% of components come from untrusted vendors. 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 RAN when equipment also from untrusted vendors have already been installed. However, the costs of subsequent rip and replace – at least of sensitive 'core' network components – may be prohibitive (i.e. equipment from untrusted vendors in the core is not actually an option for the Italian MNOs).

The Italian government has ambitions to host the first fully realised 5G network among larger European countries. Italy was the first EU country to auction 5G spectrum to MNOs, concluding 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.[130]

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, 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).

129 The National Cybersecurity Agency of France (ANSSI), the Electronic communication and Post Regulation Authority (ARCEP), and the National Agency of Frequencies (ANFR)

130 Theoretically this central actor will be OpenFiber who built the majority of the rural and currently low-market profile fiber network (a separate fiber 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 densely frequented open spaces or large closed spaces intended for commercial activities, leisure, and sport (stadiums) or health infrastructure (hospitals). The wholesale model and its leadership is nowadays at the center of the political discussion, with both technical and business matters on the table.

Additionally, Italian MNOs must abide by plans for the National Cybersecurity Perimeter (NCP) and they must test the processes, technologies and software in a National Evaluation and Certification Center *(Centro di Valutazione e Certificazione Nazionale – CVCN- L. 105/2019 and 133/2019)*. The frameworks can be stringent and costly because each MNO requires its own NOC, and the NCP requires the establishment of a National Evaluation and Certification Centre in 2021 to which MNOs will submit plans.

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.

9.2.4 Portugal

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

The Portuguese Government has ambitious plans to foster a flourishing 5G sector in the country. Initial plans were to have 90% of the population covered by 2025. Progress and governance of that process has, however, been delayed by legal challenge by established MNOs against the Portuguese regulator ANACOM. A planned EUR 237.9 million auction of spectrum and installation of equipment by untrusted vendors may yet proceed outside of an agreed framework. All three major MNOs (NOS, Vodafone and MEO) and two smaller MNOs will bid to acquire spectrum blocs in the upcoming auction, alongside new entrants and foreign bidders who will enjoy special conditions as challenging bidders. The three largest MNOs have stated they will not buy from untrusted vendors for their Core Network infrastructure, although no commitment has been made with regards to their RAN.

Portugal's approach diverges from most western European states. The Portuguese government has not legislated to manage the risks posed by, or to exclude, untrusted vendors, despite pressure from the European Commission. The Government's approach appears to be management of risk through equipment certification and approval. However, on 7th February 2020, the government mandated the establishment of a taskforce within the High Council for Cyberspace Security (CSSC) to ensure implementation of future regulatory tools, to develop a roadmap for cybersecurity involving 5G networks, and to act as a senior monitor of risk and risk management.

9.2.5 Summary

Untrusted vendors will likely continue to feature in hybrid 4G/5G core networks and 5G RANs in the absence of regulations to replace existing 4G infrastructure and of restraining the use of untrusted vendors in 5G networks.

Table 9: Likely future presence of untrusted vendors in 5G infrastructures

	Presence of untrusted vendors in MNO infrastructure			
	MNO	**4G**	**5G Core**	**5G RAN**
Germany	Deutsche Telekom Vodafone Deutschland Telefonica Deutschland 1&1 Drillisch Netz	Yes Yes Yes X	No No No Unclear	Expected Expected ORAN ORAN
France	Orange France Free Telecom France Bouygues Telecom France SFR France	No No Yes Yes	No No No No	No No Yes Yes
Italy	WINDTRE Vodafone TIM Fastweb Iliad	Yes Yes Yes Yes No	No No No No No	Yes Yes No No No
Portugal	Vodafone Altice NOS	Yes Yes Yes	No No No	TBD Expected Expected

Source: own Illustration.

9.3 Change of supply: the costs of banning untrusted vendors in each country

Costs of banning untrusted vendors for MNOs and national economies are not insignificant, but pale compared to the magnitude of future obvious and hidden costs of untrusted 5G networks .

Reliance on proprietary, untrusted vendor products in legacy telecommunications networks makes it financially attractive for MNOs to continue to work with those vendors on 5G, at least in the short-term. Banning untrusted vendors in a country is projected to cost MNOs more money investing in more expensive trusted vendors' infrastructure than the baseline scenario, and maybe causes delays to rollout of 5G services.

As we saw in Chapter 6, there are two major quantifiable cost effects of a ban. These are, firstly, the 'price effect' – increased cost to MNOs, passed on in customer bills – and secondly, the 'growth / welfare effect' – the cost of customers losing productivity benefits and a lower growth of GDP by awaiting access to 5G. An original study into these costs was beyond the scope of this project, and so we draw partly on the Oxford Economics study 'Restricting Competition in 5G network equipment throughout Europe'[131] commissioned by Huawei – and its central scenario, as a baseline. However, we find some of the underlying assumptions of this study unrealistic and the **conclusions overstated**. In general terms we assume:

1. Competition on equipment prices should remain fierce even if the number of system vendors of 5G network technology is reduced;

131 Oxford Economics (2020).

2. Availability of OpenRAN reduces MNO dependence on single vendors; increasing MNO bargaining power with a downward effect on prices;[132]

3. European MNOs revenues may be higher than had been anticipated[133], and MNOs may increase prices to consumers more modestly;[134]

4. Factors like COVID-19, legal disputes, regulatory delays, politics, appear to be causing far greater delays to 5G introduction than the time required to switch to trusted vendors;[135]

5. Delays may matter very little – the demand for machine-to-machine use cases, which will drive the greatest share of 5G-related GDP gains, is unlikely to rise until the mid-2020s.[136]

With these points in mind:

- In **Germany**, the 'central scenario' of the Oxford Economics report describes increased costs of around **EUR 479 million** per year for MNOs to build 5G networks with trusted vendors. This means that, when you break it down to the current number of existing mobile phone contracts, no more than **EUR 3.18 per contract**.[137] Oxford Economics also calculates lost GDP of around **EUR 6.9 billion** – or **EUR 83 per capita**[138], by 2035.

- **France**, a smaller telecommunications market, faces a similar **price effect** of **EUR 447 million** per year, or approximately **EUR 5.81 per phone contract.**[139] This is surprising, given that Huawei will have only a little less than 20% of the infrastructure market in France. For Oxford Economics, France faces a larger potential loss of GDP than Germany, of **EUR 7.3 billion** by 2035, or **EUR 106.09 per capita**.[140] However, French telecoms chiefs also see little impact to productivity if 5G deployments are delayed by two to three years, as demand for 5G services.[141]

- In **Italy**, according to Oxford Economics, customers face a price effect of around **EUR 282 million** per year, translating again to no more than **EUR 2.74 per contract**.[142] However, Italian MNOs interviewed have stated that switching to trusted 5G vendors will be cheaper than was expected in 2019 and their market shares will not be affected by exclusions of untrusted vendors.[143] An Ericsson report estimates that MNOs will also grow their revenues by 2030. The country may face lost GDP of around **EUR 4.7 billion** by 2035, which we calculate as **EUR 77.87 per capita**.[144]

- Lastly, **Portugal** – the smallest market and least advanced with 5G – faces a **price effect** of around **EUR 63 million, or EUR 5.29 per phone contract**.[145] Over **EUR 500 million** could be permanently **lost from GDP** by 2035, **or EUR 8.28 per capita.**[146] However, 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.[147] Government-driven delays to 5G spectrum auction and regulation are almost certain to be the systemic issue, rather than shifts to new vendors.

Even if European MNOs were permitted to install untrusted products, **working with such vendors is unlikely to remain financially attractive in long term.** 'Dumping' of cheap products by these firms could be part of a strategy to force Nokia and

132 BIGS, Country Study Germany.
133 Ericsson (2019).
134 Wagener (2020).
135 Confirmed by BIGS and partners' interviews with MNO leaders, conducted for the detailed country studies behind this chapter.
136 Confirmed by BIGS and partners' interviews with MNO leaders, conducted for the detailed country studies behind this chapter.
137 We divide the price effect by numbers of SIM cards within the economy. Germany had around 150m active SIM cards in 2020.
138 Based on the 2019 population of 83.02m people.
139 France had around 96.2m active SIM cards in 2020, including M2M applications.
140 Based on the 2019 population of 68.8m people.
141 Public statements and interviews by SystemX.
142 Italy had around 103.7 million active SIM cards in 2020.
143 Italy Country Study, by CEFRIEL
144 Based on the 2019 population of 60.36m people.
145 Portugal had around 17.1 million active SIM cards in circulation in 2020
146 Based on the 2019 population of 10.29m people.
147 Rollout in Lisbon and Porto regions will mean 5G rapidly reaches around 50% of the population.

Ericsson to exit the 5G market, restricting competition, and raising the prospect of MNOs **locked in** with untrusted vendors then free to raise prices in future. Thinking long-term, MNOs will also need to upgrade to 6G in the future, while Chinese firms will have little incentive to keep prices low. This is probably the preferred situation for Chinese firms, as indicated by them having shown little interest in integrating OpenRAN standards (allowing equipment from multiple vendors to interoperate in one 5G network).


Foto © sdecoret/iStockphoto

9.4 Obvious Costs of Untrusted Vendors by Country

Compromised 5G networks could cost national economies tens of billions in the event of interstate tension or conflict with China.

Before moving on to hidden costs, it is useful to consider the obvious costs of having allowed national networks to be overly vulnerable to attack and interference by foreign powers. As Chapter 5 describes, assessing obvious costs arising under 'normal' scenarios is difficult.[148] However, it is possible to examine obvious costs that may occur during severe geopolitical tension in two ways.

The **first approach** is to consider the financial impacts of several days' total network outages – and **shutdown of the economy** – on GDP. With this frame of reference, as Europe's largest economy, with a GDP of approximately EUR 3.5 trillion in 2019, **Germany** could face severe costs.[149] With a lost working day amounting to around EUR 4.31 billion, a **three-day shutdown** therefore costs around **EUR 12.94 billion**, and a **six-day shutdown** costs **EUR 25.88 billion**, or almost 0.75% of GDP. It seems inconceivable that network services could be fully restored in a matter of days.

148 Tangible and intangible effects of subtle attacks designed to steal or manipulate data, the effects of 'slow burn' espionage, and the long-term slow down – 'throttling' – of networks by an adversary is extremely complex to cost. Across multiple countries is even more challenging, as starting assumptions will be complex and contrived to allow comparison.

149 Statistisches Bundesamt (2020).

This is particularly the case, when a switch of the technology is necessary, as the scale of rip and replace required across Germany is vast.

A **second approach** is to consider 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 – as listed below – according to their severity, and to better illustrate 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, and mobile internet services.

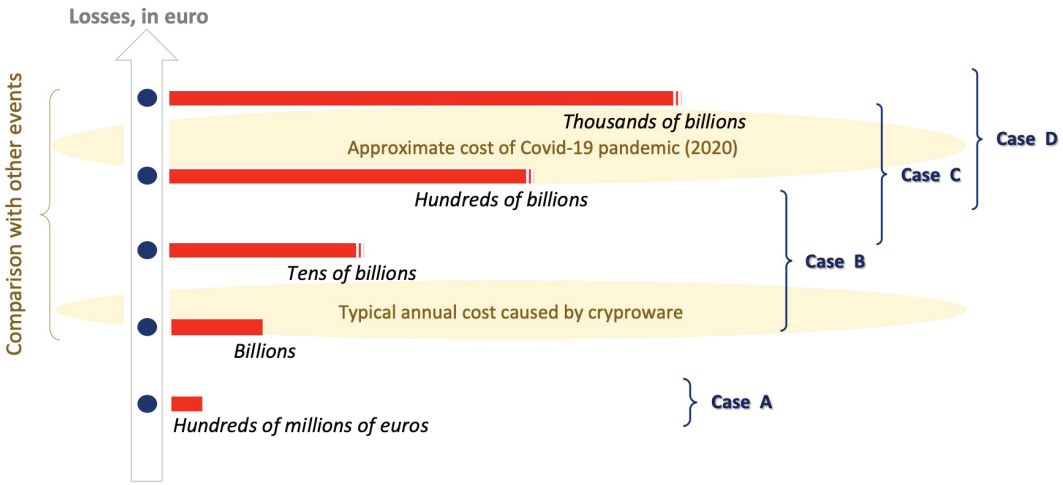
Case B – The blockade also affects the IoT, industrial uses (Factory 4.0…), or communicating vehicles.

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, medical and industrial disasters.

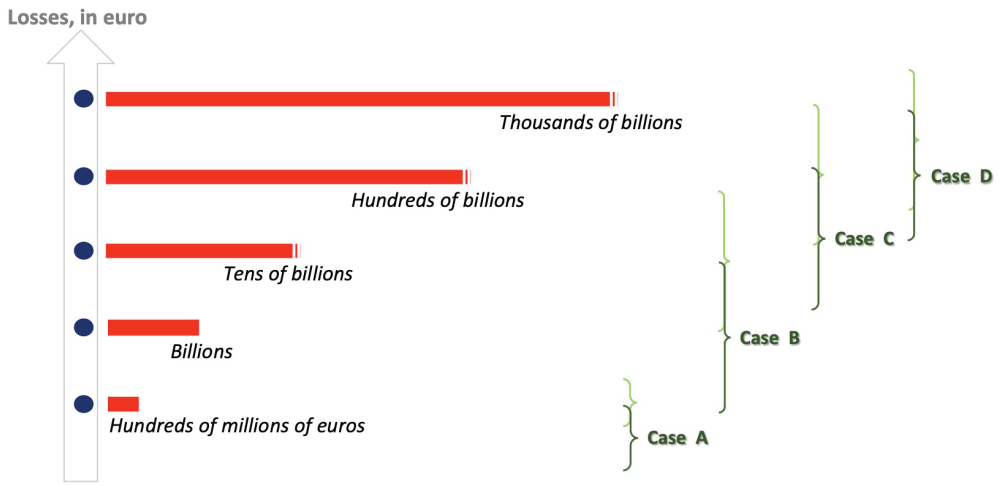
The method was developed for France so other countries are compared against it. As economies of similar size, **France** and **Italy** are likely to suffer similar losses against each of the cases:

Figure 4: Scale of harm for France and Italy (euro)



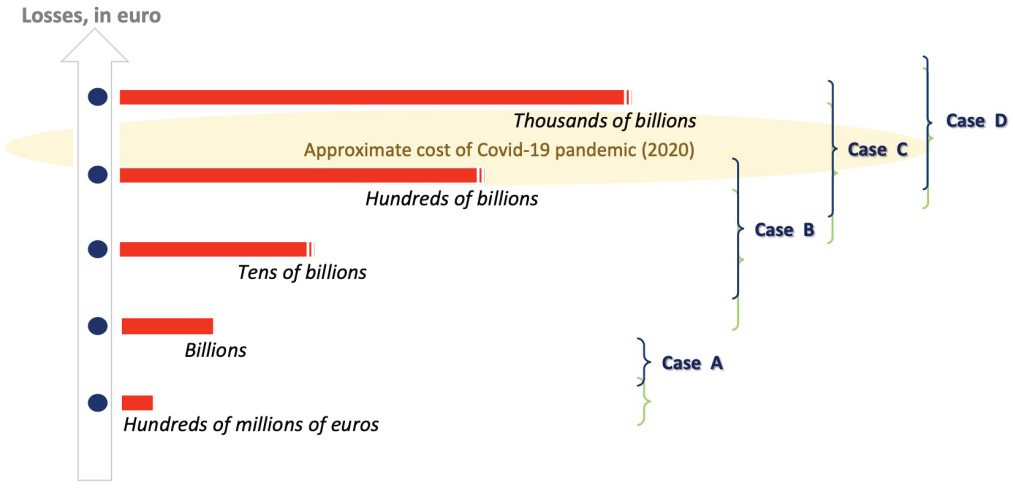
As the smallest economy, **Portugal** is likely to suffer the least in absolute terms, but not insignificantly relative to its size. (France is in light green)

Figure 5: Scale of harm for Portugal (euro)



As the largest economy with the greatest role being played by untrusted vendors, **Germany** can expect to incur the greatest costs. (France is in light green)

Figure 6: Scale of harm for Germany (euro)



9.5 The hidden costs of untrusted 5G Vendors

The report now outlines the hidden costs of remaining with untrusted vendors for Germany, France, Italy and Portugal, having covered the costs of parting ways with untrusted 5G vendors and obvious costs from manipulation of untrusted infrastructures during international strife or even war.

9.5.1 Test Centres

Centres for the assessment and certification of 5G hardware, software and network operation should cost the largest economies' taxpayers almost EUR 60 million per year to operate

As we argued in Chapter 6, 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, and because the networks and the technology is now 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 testbed and digital 'twin' networks to understand when the real network could be being abused.

Accurately costing government test centres is challenging.[150] Equating costs spent to full scrutiny and assurance of vendors' products is also problematic. Magnitude of costs is likely to depend on the required level of scrutiny and simulation of equipment and network functions. In absolute terms, responsibilities (determined by national legislation), salary and capital costs are the key determinants. A simple 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. In the UK, the independent Huawei Cyber Security Evaluation Centre is actually funded by Huawei, but managed and scrutinised by an oversight board including the UK Government National Cyber Security Centre.

We estimate Germany's National Test Centre could cost up to EUR 60 million. Based on estimates of the size of the market and the scale of untrusted vendors' role in each market, France's Test Centre could cost as much as EUR 30 million, mainly due to staff costs, with a need for about 150 experts and administrative staff; Italy's, EUR 40 million, and Portugal's, EUR 20 million, an estimate that would place the Portuguese Test Centre in the cost vicinity of other reference R&D centres in the country, such as INESCTEC.

9.5.2 Costs of data breaches

Data breaches in larger economies substantially reliant on untrusted vendor infrastructures could cost billions of EUR.

Data breaches (exfiltration of data) are a fact of life in communications networks, especially those spanning entire countries. In offering estimates for the 'hidden costs' of data breaches in the 5G future, we are in fact estimating national annual costs of projected quantities of data breaches that could be expected to occur while data is in transit across networks operated by untrusted vendors. We conjecture potential growth rates in cybercrime activity on data in transit and growth rates in the cost of data breaches, use available assumptions of the penetration of 5G infrastructures into western European infrastructures (as a proportion of total data transmission volumes), and the proportion of that which can be expected to use untrusted vendor infrastructures. Estimates are likely to be understated, as accounting for the growth of machine-to-machine requirement for traffic volumes is extremely challenging.

- In **Germany**, annual costs of data breaches stemming from the presence of untrusted vendors in 5G networks could be as high as **EUR 18 billion** by 2024. Such a large market nat-

150 We can employ both top-down costing techniques (looking at analogous Centres) and bottom-up costing techniques (employing estimates of the cost of processes such as software review, supply chain audits, and network monitoring costs by time).

urally has a huge volume of communications, of which more than a quarter (29%) we expect to see over 5G networks by 2024 – and 50% of that 29% could take place over untrusted networks, unless the IT Security Law 2.0 has the effect of keeping untrusted vendors out of the network.

- For **France**, we estimate annual costs in the region of **EUR 623 million** by 2024. The proportion of traffic carried by untrusted 5G networks is likely to be lower than in Germany and Portugal, with untrusted vendors likely to have less than a 20% market share, covering mainly rural areas. However, the number of reported data breaches in Figure 3 is unrealistically low for France. In the alternative, we have therefore assumed in a second calculation that the number of data breaches is comparable to that of Germany. In that case the costs would be in the region of **EUR 4.5 billion**.

- In **Italy**, we estimate annual costs of data breaches of around **EUR 580 million** by 2024 when using the same approach with the same data sources. 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 Italy. 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, by 2024 if the current market share is confirmed. Also, the number of reported data breaches in Italy is unrealistically low (see Figure 3), and the average cost of a data breach is smaller with respect to Germany.

- In **Portugal**, the smallest market, we estimate annual **costs of data breaches by 2024 of around EUR 133 million**.[151] Using official data from the National Cybersecurity Centre for the last 5 years, we believe cybercrime on data in transit for Portugal will increase at a higher rate than the global average.[152] However, we also estimate a lower volume of traffic will be handled by untrusted vendors' equipment than Germany (30% compared to 50%+) because untrusted vendors are not so dominant in Portuguese 4G infrastructure or 5G infrastructure plans.

Table 10: Projected growth in national costs of data breaches occurring over untrusted 5G network

	Costs, in million €		
	2022[153]	2023	2024
Germany	16,399.44	16,272.34	18,009.26
France	567.31	562.91	623.00
France[154]	4,142.77	4,110.66	4,549.43
Italy	528.28	524.48	580.46
Portugal	96.72	107.25	132.65

Source: own Calculation.

151 Since no data on cost per breach is available for Portugal, we assume that since both Portugal and Italy's ICT industries report similar percentages of value added relative to GDP, both countries' maturity in response and capacity would be similar, and the difference in cost of breach would be proportional to the size of both countries GDP's – Portugal circa 12% of its Italian counterpart.

152 CNCS (2020), p. 40.

153 Calculated from US Dollar values at an exchange rate of 0.82€ to the dollar.

154 In this calculation we assume that France has proportionally to it's size the same data breaches as Germany. Nevertheless, France has still a much smaller dependency on untrusted networks, which is why the cost are still expected to be much lower than for Germany.

9.5.3 Loss of security-sensitive clients – shift of commercial demand.

Some European MNOs should factor in a substantial shift of their customers moving to MNOs using trusted suppliers of 5G infrastructures. Tax revenues and jobs could be affected if customers emigrate.

In Chapter 6, we described how to estimate hidden costs to MNOs caused by security-sensitive clients taking their business to other MNOs, and even to other countries. In summary, we calculate the proportion of MNO revenues arising from security-sensitive business clients' use of mobile telecommunications services.[155] We use the GDP share of critical infrastructure providers and of IPR intensive companies as an approximation for security sensitive customers.

This shift of demand will decrease some MNO's profits and may even cause welfare losses for all of society, depending on whether clients shift MNO or shift their entire production to countries with more secure networks. Figures may also increase, as future regulations and challenges acquiring insurances could see even clients' suppliers cease using untrusted 5G networks.

- In **Germany** the share of critical infrastructure providers of GDP is 27%. The share of IPR-intensive value creation is almost 50%. We therefore estimate that more than half of the market with business customers or **EUR 4.6 billion** will have a tendency to shift toward MNOs with only trusted technology in their 5G networks. The costs for Germany are significantly higher compared to the three following countries, because of a wider definition of KRITIS and a higher share of both critical and IPR-intensive companies.

- In **France**, we estimate **shifting demand** worth more than **EUR 1.2 billion** in a market worth EUR 30.7 billion in 2020. Mobile telecommunications services made up a similar share of revenues as in Germany (43%, vs. 44% in Germany), but business use is a little under half that in Germany (18% of that 43%), with as much of 50% of business clients coming from the KRITIS and IPR intensive sectors. Moreover, operators using untrusted equipment represent only a third of the business market.

- In **Italy**, we estimate more than half or **EUR 1.34 billion** of revenue with commercial customers in the telecommunications market may be at stake from shifting towards trusted networks. Italy's 2020 market (EUR 31.58 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.

- In **Portugal**, the commercial telecommunications market may see **shifting demand worth up to EUR 324.2 million (or 40%)**. This figure may grow as Portuguese regulation for industrial cyber-security of sensitive sectors catches up. Portugal is the smallest telecommunications market amongst the four countries (EUR 3.55 billion in 2020), albeit with the largest sub-market for mobile telecommunications services, but with a very narrow definition of what is considered a critical infrastructure.[156]

9.5.4 Loss of security-sensitive clients – shift of government demand and redundant infrastructure

Governments may need to spend almost €700m to create secure, redundant networks if they can't trust MNOs using untrusted vendors' equipment.

Governments have one further option open to them to ensure the security of the networks on which they rely: build their own. Naturally, this is extremely expensive, and will depend on the scale, number of nodes, security requirements, the functions it needs to perform, and also comes with an overhead for a state communications provider, or at least sub-contracted MNOs, to operate it. We can

155 Where internal MNO, government and commercial information on proportion of revenues from, or spend of, these clients is not available, we use relevant values such as the proportion of security-sensitive industries' contribution to national GDP, as reasonable assumptions to aid our calculations of the share of revenues from these clients.

156 Security-sensitive clients form the lowest share (20%) of the telecommunications market of the four countries we surveyed, though this may be because Portugal's definition of KRITIS sectors is very narrow.

estimate costs using 'top down' methods looking at existing projects and analogous initiatives from the recent past.

- For **Germany**, a national contingency network – the Netz des Bundes – is already costing the government (taxpayer) **in excess of EUR 426 million** to implement. Annual operational costs would also be incurred at around EUR 92 million per year. Original German Federal estimates did, however, indicate that an external operator would cost the taxpayer EUR 160 million per year.

- For **France**, we estimate that the redundant communications network currently in operation has already cost even more than in Germany, potentially as much as **EUR 470 million or even more.**

- For **Italy**, we estimate the country will have to invest as much as **EUR 700 million**. 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/CHF, radio, TETRA etc). Out of these, the calculation considered those that will be substituted by 5G in the future, according to interview, despite no official plans having been announced.

- **Portugal** has already invested **EUR 450 million** in a national emergency telecommunications company, SIRESP, partly owned by the Portuguese government. It requires around EUR 25 million worth of robustness and security improvements in the 550-antenna network to bring it up to contemporary standards. Portugal pays Altice and Motorola EUR 30 million per year to operate it.

9.5.5 Costs of Rip & Replace

MNOs and Governments leave themselves open to liabilities of billions of EUR, if major data losses or interstate conflict requires rip and replacement of untrusted 5G networks.

'Rip and replace' is a cost for MNOs and possibly their consumers, a requirement generally arising out of changes in national legislation. We are already seeing rip and replace mandated for Bouygues and SFR in France. Rip and replace will undoubtedly be required following major service outages or attacks facilitated through untrusted vendors.

Costs depend on the size of the state, the entrenchment of untrusted vendors in infrastructure, and the timespans over which rip and replace is required. For example, short-term hasty rip-and-replace after malicious interference or service outages is likely to be far more expensive than long-term, orderly rip and replace required by legislation. To replace 5G infrastructures is a cost that will continue to escalate the more untrusted vendors' equipment is embedded in a national 5G infrastructure. For initial estimates, we have used quoted figures from MNOs and existing reports. The figures do not cover additional indemnities caused.

Dt Telekom claims that it would cost them around **EUR 3 billion to rip and replace untrusted vendor equipment**.[157] This is a number we can't verify, but it seems to gravely exaggerate the costs of switching to a trusted vendor. For example, British Telekom, which also relied very much on Huawei technolog y, now quotes the cost of a full ban at just £500 million.[158] It certainly ignores costs that would occur later in the lifecycle if they do not switch to trusted vendors. And, of course, an MNO ignores the costs that must be borne by others.

In **France**, we can **expect costs of up to EUR 1 billion**, reflecting a slightly smaller market size and the dominance of Ericsson and Nokia infrastructures.[159] In **Italy**, we expect costs of around EUR 600 million, from a study produced in 2019[160]. For **Portugal** we could not find a similar estimate for the cost for replacing untrusted technology from 4/5G networks.

157 Handelsblatt (2020).
158 Reuters (2020).
159 Le Figaro (2020).
160 Bechis (2020), Istituto Affari Internazionali (2020).

REFERENCES

5G PPP Security WG (no year): "5G PPP Security Phase 1 Security Landscape", https://usermanual.wiki/Document/5GPPPWhitePaperPhase1SecurityLandscapeJune2017.809074850/view, accessed Dec. 2020.

Akerlof, George A. (1970), „The Market for ‚Lemons': Quality Uncertainty and the Market Mechanism". Quarterly Journal of Economics. The MIT Press.

ASPI (2020): "ICT for Development in the Pacific Islands", https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-02/ICT%20for%20development%20in%20the%20Pacific%20islands.pdf?x_oS.r8OVVfTlxxgNHI58k_VL45KC83H

Behesti, B. (2019): "What 5G means for smart cities", London, https://www.smartcitiesworld.net/opinions/opinions/what-5g-means-for-smart-cities , accessed Oct 2020.

Berzina, Kristine (2020): 5G Security: The New Energy Security. Europe's Strategic Vulnerabilities in the 5G Era and Lessons Learned from Europe's Dependence on Russia's Natural Gas. https://securingdemocracy.gmfus.org/5g-energy-security , accessed Nov 2020.

Bischoff, P. (2020): "How data breaches affect stock market share prices", Kent, https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/, Accessed Oct. 2020.

Bitkom (2018): "Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie", Studienbericht 2018, https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf, accessed Aug. 2020.

BMI (2020): "Bundesministeriums des Innern, für Bau und Heimat: Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0), 19. November 2020, Berlin.

BMWi (2018): "KfW erwirbt im Auftrag des Bundes temporär Anteil am deutschen Übertragungsnetzbetreiber 50Hertz", https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2018/20180727-kfw-erwirbt-im-auftrag-des-bundes-temporaer-anteil-am-deutschen-uebertragungsnetzbetreiber-50hertz.html, accessed Oct. 2020.

Brookings Institution (2017): „Global digital trade 1: Market opportunities and key foreign trade restrictions". Testimony of Joshua P. Meltzer before the United States International Trade Commission, April 12, 2017, https://www.brookings.edu/testimonies/global-digital-trade-1-market-opportunities-and-key-foreign-trade-restrictions/, accessed Dec. 2020.

Bretschneider, W., Freytag, A., Rieckmann, J., Stuchtey, T. (2020): Sicherheitsverantwortung zwischen Markt und Staat – eine institutionentheoretische Analyse, in: ORDO, Vol. 70 Nr. 1, S. 89 – 124.

BSI (2020): "Zertifizierung und Anerkennung", Bonn, https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/ITSEC_CC/CC_Liste/CC_Liste_node.html, accessed Oct. 2020.

Bughin, J. et al (2016): "Digital Europe: Pushing the Frontier, Capturing the Benefits", McKinsey Global Institute, June 2016.

Bundesnetzagentur (2020): "Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG) Version 2.0", pp. 9 – 10, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=3 , accessed Nov. 2020.

Bundesamt für Verfassungsschutz (2019): "Verfassungsschutzbericht 2019", https://www.verfassungsschutz.de/embed/vsbericht-2019.pdf

Busse, M. and C. Hefeker (2007): "Political risk, institutions and foreign direct investment". European Journal of Political Economy 23, 397-415

Cave, D. (2020): "5G matters: (Geo)politics and critical national infrastructure", https://www.orfonline.org/expert-speak/5g-matters-geopolitics-critical-national-infrastructure-60548/, accessed October 2020.

Cerulus L. (2019): "How Ukraine became a test bed for cyberweaponry", https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/, accessed Oct 2020.

CNCS (2020), "Ciberseguranca em Portugal – Riscos & Conflitos", https://www.cncs.gov.pt/content/files/relatorio_riscos.conflitos2020__observatoriociberseguranca_cncs.pdf, accessed Dec. 2020.

Commission ad hoc Cyber Risk (2018): "Assurer le risque cyber - Rapport du Club des juristes", https://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_assurer-le-risque-cyber_janvier_2018_fr-2.pdf, accessed Nov 2020.

Cotelle, P., Wolf, P., Suzan, B., Santoni, J.L., Lemerle, L. et al. (2019): "Maîtrise du Risque Cyber et Assurance : Scénario cyber s'appliquant à la filière aéronautique Réponse du marché", Rapport de recherché, IRT SystemX.

Cotelle, P., Wolf, P., Suzan, B. (2015): "Cyber Risk and Insurance Cyber Risk Governance throughout the value chain and its transfer to the Insurance", Cyber Risk and Insurance, https://www.irt-systemx.fr/wp-content/uploads/2017/01/ISX-IC-EIC-transfert-risque-LIV-0401-v10_2016-10-25-ang-v2.pdf, accessed Oct. 2020.

Crawford, N. (2020): "Defending against economic statecraft: China, the US and the rest", https://www.iiss.org/blogs/analysis/2020/10/economic-statecraft-china-us,accessed Oct 2020.

CrowdStrike (2019): "CrowdStrike Report Reveals Cyber Intrusion Trends from Elite Team of Threat Hunters", October 9, 2019, at https://www.crowdstrike.com/resources/news/crowdstrike-report-reveals-cyber-intrusion-trends-from-eliteteam-of-threat-hunters/, accessed Oct 2020.

Defense Science Board (2019): "Defense Applications of 5G Network Technology", https://www.hsdl.org/?abstract&did=828623#:~:text=From%20the%20Executive%20Summary%3A%20%22Emerging,4G%20%5Bfourth%20generation%5D%20networks,accessed October 2020.

Demer, John C. (2018): U.S. Department of Justice, Statement of John C. Demers, Assistant Attorney General, National Security Division, U.S. Department of Justice Before the Committee on the Judiciary, United States Senate, December 12, 2018, at https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20Demers%20Testimony.pdf

Department of Defense (DoD). (2020): "Department of Defense (DoD) 5G Strategy", https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf , accessed Oct 2020.

Deutsche Bundesbank (2012): "Kalendarische Einflüsse auf das Wirtschaftsgeschehen", Monatsbericht Dezember, p.59.

DG Connect (2020), "Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures". https://ec.europa.eu/digital-

single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures, accessed Oct. 2020.

DLA Piper (2020): "DLA Piper GDPR data breach survey 2020", https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/, accessed Dec. 2020.

Ekudden, Erik (2018): "Five Technology Trends Augmenting the Connected Society", in: Ericsson Technology Review, September 10, 2018, https://www.ericsson.com/48f8e0/assets/local/reports-papers/ericsson-technology-review/docs/2018/technology-trends-2018.pdf.

Endgadget (2020): "Huawei tested facial recognition that targeted Uyghurs in China". December 8, 2020, https://www.engadget.com/huawei-facial-recognition-uyghurs-172304197.html?guccounter=2 , accessed Dec. 2020.

Ericsson (2019): "What role will Artificial Intelligence have in the mobile networks of the future?", https://www.ericsson.com/en/networks/offerings/network-services/ai-report, accessed Oct. 2020.

Ericsson (2020a). "Security in 5G RAN and Core deployments", https://www.ericsson.com/49a5ea/assets/local/reports-papers/white-papers/ericsson-whitepaper-5gran.pdf, accessed Nov. 2020.

Ericsson (2020b): "TDC Denmark goes live with Ericsson 5G", https://www.ericsson.com/en/news/2020/9/tdc-denmark-goes-live-with-ericsson-5g, accessed Oct. 2020.

Ericsson (2020c): "5 Key Facts About Radio Access Networks", https://www.ericsson.com/en/public-policy-and-government-affairs/5-key-facts-about-5g-radio-access-networks, accessed Oct. 2020.

ENISA (2018): "Signaling Security in Telecom SS7/Diameter /5G", https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g/at_download/fullReport, accessed Oct. 2020.

EU Commission (2020): Commission Staff Working Document, "Report on the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks", SWD (2020) 357 final.

European Union Agency for Cyber Security (ENISA) (2019): "Threat Landscape for 5G Networks", https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks, accessed Oct 2020.

European Union Intellectual Property Office (EUIPO) (2019): "Impact of intellectual property rights intensive industries in the European Union", https://euipo.europa.eu/ohimportal/en/web/observatory/ip-contribution, accessed Nov 2020.

Federal Council (2016): Draft law of the Second Law of Adaptation of the Federal Agency for Public Safety Digital Radio (BDBOS), printed matter 786/16 (new).

Federal Law Gazette (2020): "Act on the Adoption of a Second Supplement to the Federal Budget for the Financial Year 2020", (Second Supplementary Budget Act 2020), pp.12,14,16.

Financial Times (2020a): "China's biggest chipmaker SMIC hit by US sanctions", https://www.ft.com/content/7325dcea-e327-4054-9b24-7a12a6a2cac6?shareType=nongift, accessed Oct. 2020.

Financial Times (2020b): "Germany crackdown set to exclude Huawei from 5G rollout", https://www.ft.com/content/35197477-acef-4429-a1d8-71743ee8d8e3, accessed Oct 2020.

Fraunhofer IIS (2020): "Staatsminister Aiwanger eröffnet 5G Bavaria-Testzentrum und das Testbed-Industrie 4.0 am Fraunhofer IIS", Erlangen, https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf, accessed 2020.

Gambetta, Diego (1988): 'Can We Trust Trust?' in: D.G. Gambetta (ed.) Trust, New York: Basil Blackwell: 213–37.

German Federal Court of Auditors (2017): "Annual Report 2017", Audit results related to individual plans Federal Ministry of the Interior, Remarks No. 04 pp.2, https://www.bundesrechnungshof.de/de/veroeffentlichungen/produkte/bemerkungen-jahresberichte/jahresberichte/2017/einzelplanbezogene-pruefungsergebnisse/bundesministerium-des-innern, accessed Oct 2020.

Gilli, A & Bechis, F. (2020): "NATO & the 5G Challenge", https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html , accessed October 2020.

Globaltrademag.com (2020): Unpacking US-China Sanctions and Export Control Regulations: Huawei. Sept. 10, 2020, https://www.globaltrademag.com/unpacking-us-china-sanctions-and-export-control-regulations-huawei/, accessed Oct. 2020.

GSMA (2019): „The 5G Guide – A Reference for Operators", https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf, accessed Nov 2020.

Hammami, H., Hammami, M., Coulibaly, S., & Marzouk, M. (2020): "Determinants of FDI attractiveness: A MCI model approach". Economics Bulletin, 40(2), 1033-1048.

Handelsblatt (2014): "Bund baut Kommunikationssystem um", Handelsblatt from the 26th June, https://www.handelsblatt.com/politik/deutschland/nach-nsa-affaere-bund-baut-kommunikationsnetz-um/10114010.html?ticket=ST-1479718-bbBLRnwCBzeAYJsKvdb0-ap2, accessed Oct. 2020.

Handelsblatt (2020): „„Armageddon"-Szenario: Telekom spielt Huawei-Bann durch", https://www.handelsblatt.com/technik/it-internet/ausschluss-von-netzausruester-armageddon-szenario-telekom-spielt-huawei-bann-durch/25918402.html?ticket=ST-2101572-caqXUFPkiY5AFBKX0pz2-ap4, accessed Nov. 2020.

Hansen, A. und Meyer, D. (2018): "Wie viel kosten uns die arbeitsfreien Feiertage?", ifo Schnelldienst Kommentar, März, p.18.

Herpig, Sven (2020): Understanding The Security Implications Of The Machine-Learning Supply Chain. Available at: https://www.stiftung-nv.de/sites/default/files/understanding_the_security_of_the_machine-learning_supply_chain.pdf, accessed Oct. 2020., accessed Oct. 2020.

Holland, M. (2014): "NSA-Skandal: Auch Bundestag beendet Kooperation mit Verizon", https://www.heise.de/newsticker/meldung/NSA-Skandal-Auch-Bundestag-beendet-Kooperation-mit-Verizon-2241967.html, accessed Oct 2020.

Hui, X et al. (2020): "5G network-based Internet of Things for demand response in smart grid: A survey on application potential", Applied Energy, Vol. 257. https://www.sciencedirect.com/science/article/pii/S0306261919316599 , accessed Oct. 2020.

IBM (2020): "Cost of a Data Breach Report", November 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/ , accessed Dec. 2020.

Information is beautiful (2020): "Codebases – Millions of lines of code", https://informationisbeautiful.net/visualizations/million-lines-of-code/, accessed Oct 2020.

International Telecommunications Union (ITU) (2018): "Setting the Scene for 5G: Opportunities & Challenges", Switzerland, https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf

ITU (2019): „Financial Inclusion Global Initiative (FIGI)", Report of Security Workstream, https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Technical%20report%20on%20the%20SS7%20vulnerabilities%20and%20their%20impact%20on%20DFS%20transactions.pdf, accessed Oct. 2020.

Jornaldenegocios (2020): "Centeno: Queda do PIB é de 6,5% por cada 30 dias úteis com economia parada". https://www.jornaldenegocios.pt/economia/detalhe/centeno-queda-do-pib-e-de-65-por-cada-30-dias-uteis-com-economia-parada , accessed Dec. 2020.

Kavanagh, S. (n.a): "What is Enhanced Mobile Broadband?", United Kingdom, https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/ , accessed Oct 2020.

Kim, B. (2019): "ICT-Based Business Communication with Customers in the 4th Industrial Revolution Era", Business Communication Research and Practice, 2(2), p. 55-61.https://doi.org/10.22682/bcrp.2019.2.2.55 , accessed Oct. 2020.

KPMG (2019): "Cloud-Monitor 2019 - Public Cloud und Cloud Security sind kein Widerspruch", https://hub.kpmg.de/cloud-monitor-2019, accessed Oct. 2020.

Lee, J. (2019): "The National Security Risks Over Huawei and its 5G Network: Is an Outright Ban or a Restricted Access the Answer?", Oxford, https://www.law.ox.ac.uk/research-subject-groups/commercial-law-centre/blog/2019/05/national-security-risks-over-huawei-and, accessed Oct. 2020.

Le Figaro (2020): "5G sans Huawei: l'État négocie avec les opérateurs", 6.3.2020, https://www.lefigaro.fr/secteur/high-tech/5g-sans-huawei-l-etat-negocie-avec-les-operateurs-20200306#_=_, accessed Dec. 2020.

Le Maistre, R. (2020): "Rakuten, Telefónica join forces on Open RAN developments", https://www.telecomtv.com/content/open-networking/rakuten-telef-nica-join-forces-on-open-ran-developments-39678/, accessed Nov. 2020.

Lewis, J. (2018): "How 5G will shape innovation and security", Washington DC, https://csis-website-prod.s3.amazonaws.com/s3fs: -public/publication/181206_Lewis_5GPrimer_WEB.pdf, accessed Oct. 2020.

Lloyds (2015): "Business Blackout: The insurance implications of a cyber attack on the US power grid", Cambridge, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf, accessed Oct 2020.

Lord, N. (2019): "Data Protection: Data In Transit vs. Data At Rest", https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest, accessed Dec. 2020.

Miller, M. (2020): "Defense Department designates $600 million for 5G testing at military sites", Washington DC, https://thehill.com/policy/technology/520288-defense-department-designates-600-million-for-5g-testing-at-military-sites , accessed Oct 2020. , accessed Oct 2020.

Nakashima, E. (2019): "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible", Washington DC, Washington Post from the 29th May, https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html, accessed Oct. 2020.

NIS Cooperation Group (2020): "Cybersecurity of 5G networks – EU toolbox of risk mitigating measures", CG Publication, January, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

Nokia (2020a): "Connected Vehicles", https://www.nokia.com/networks/5g/use-cases/connected-vehicles/ , accessed Oct 2020.

Nokia (2020b): "E-Health", https://www.nokia.com/networks/5g/use-cases/ehealth/ , accessed Oct 2020.

Nokia (2020c): "Threat Intelligence Report 2020", https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html?_ga=2.263942024.520766677.1603877763-652481011.1603877763, accessed Oct. 2020.

Normenkontrollrat (2014): „Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKRG: Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (NKR-Nr. 3044)", 4. December 2014, Berlin.

Normenkontrollrat (2016): „Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NKR-Nummer 3970, BMI)".

NCSC (2020): "Security analysis for the UK telecoms sector", Summary of findings, https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf, accessed Oct. 2020.

Okumura Y. (2019): "5G for eHealth – 5G Utilization in Telemedicine", ITU-D Study Groups Rapporteur Group meetings, https://www.itu.int/dms_pub/itu-d/oth/07/1e/D071E0000010001PDFE.pdf , accessed Oct 2020.

Owen, G. (2020): "The race to Open RAN is a marathon, not a sprint", https://www.huawei.com/en/publications/communicate/89/open-ran-is-a-marathon-not-a-sprint, accessed Oct 2020.

Oxford Economics (2020): "Restricting Competition in 5G Network Equipment Throughout Europe – an Economic Impact Study", June 2020.

Park, J.-Y., Robles, R., Hong, C.-H., Yeo, S.-S., & Kim, T.-h. (2008): "IT Security Strategies for SME's", International Journal of Software Engineering and Its Applications, Vol. 2, No. 3, July, pp. 91-98.

Ponemon Institute (2017): "The impact of data breaches on reputation and share value", https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf, accessed Oct. 2020.

Prague 5G Security Conference (2019): "The Prague Proposals", Prague, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/, accessed Oct 2020.

Prague Proposals (2019): https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf, accessed Oct. 2020.

Pupillo, L. (2019): "5G and National Security: A complex puzzle", Brussels, https://www.ceps.eu/5g-and-national-security/, accessed Oct 2019.

Reuters (2020): "BT says Huawei ban can be absorbed in 500 million pounds already earmarked", https://www.reuters.com/article/us-britain-huawei-bt-costs/bt-says-huawei-ban-can-be-absorbed-in-500-million-pounds-already-earmarked-idUSKCN24F2A2, accessed Dec. 2020.

Roke Manor Research Ltd (2020): "5G & Law Enforcement: How it could impact investigation & crime prevention", Hampshire, https://www.roke.co.uk/media/dtwinm2g/5g-law-enforcement-article-long-final-whitepaper-template.pdf , accessed Oct 2020.

Säkerhetspolisen (2020): "The importance of a secure 5G network", Stockholm, https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2020-10-20-the-importance-of-a-secure-5g-network.html?utm_campaign=21.%20october%202020%20-%20Kundeemneliste%20-%20What%20creates%20competition%20in%20the%20telecommunications%20industry%20Can%20the%20number%20of%20mobile%20operat189115&utm_source=Kundeemneliste&utm_medium=email, accessed Oct. 2020.

Shermann, J. (2019): https://medium.com/dukeuniversity/whats-the-deal-with-huawei-and-a-hack-at-african-union-headquarters-1e454c1f31a2, accessed Nov. 2020.

Sivalingum, T, et al. (2019): "Positioning of Multiple Unmanned Aerial Vehicle Base Stations in future Wireless Network", Oulu, https://www.researchgate.net/publication/335826943_Positioning_of_Multiple_Unmanned_Aerial_Vehicle_Base_Stations_in_future_Wireless_Network , accessed Oct 2020.

Smartbear (2019): "Bewährte Verfahren für die Codeprüfung", https://smartbear.com/learn/code-review/best-practices-for-peer-code-review/?lang=de-de, accessed Oct. 2020.

Statistisches Bundesamt (2020): "Federal Statistical Office: National accounts, gross domestic product 2019", Wiesbaden, https://www.destatis.de/DE/Themen/Wirtschaft/Volkswirtschaftliche-Gesamtrechnungen-Inlandsprodukt/Tabellen/bip-bubbles.html, accessed Oct 2020.

Strand Consult (2019): "The real cost to rip and replace of Chinese equipment in telecom networks", https://strandconsult.dk/the-real-cost-to-rip-and-replace-chinese-equipment-from-telecom-networks/, accessed Oct 2020.

Strand Consult (2020): "Understanding the Market for 4G RAN in Europe", https://strandconsult.dk/understanding-the-market-for-4g-ran-in-europe-share-of-chinese-and-non-chinese-vendors-in-102-mobile-networks/ , accessed Oct 2020.

Sullivan, J. and Kamensky, D. (2017): "How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid", The Electricity Journal, 30(3), pp. 30-35.

Taulli, T. (2020): "How 5G will unleash AI", https://www.forbes.com/sites/tomtaulli/2020/05/08/how-5g-will-unleash-ai/ , accessed Oct 2020.

techUK. (2019): "How can 5G technology support the emergency services?", https://www.techuk.org/insights/reports/item/15317-report-how-can-5g-technology-support-the-emergency-services , accessed Oct 2020.

The Australian Financial Review (2020) Huawei data centre built to spy on PNG. https://www.afr.com/companies/telecommunications/huawei-data-centre-built-to-spy-on-png-20200810-p55k7w, accessed Oct 2020., accessed Oct 2020.

thelocal.dk (2020): "Denmark's TDC shuns China's Huawei for 5G rollout", Stockholm, https://www.thelocal.dk/20190319/denmarks-tdc-shuns-chinas-huawei-for-5g-rollout, accessed Oct 2020.

Tomás, J. P. (2020): "Rakuten Mobile launches 5G services in parts of Japan", RCRWireless News from the 30th September, https://www.rcrwireless.com/20200930/5g/rakuten-mobile-launches-5g-services-in-parts-of-japan.

U.S. Department of Commerce (2020): Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies. Press release, May 15, 2020, https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts, accessed Oct. 2020.

UTAIL (2020): "Custa Quanto? Regulamento (EU) 2016/679 (Regulamento Geralde Proteção de Dados (RGPD))" https://www.jurisapp.gov.pt/media/1109/ail-rgpd.pdf , accessed Dec. 2020.

Voland, T. and Büsch, P. (2020): "Nächster Versuch – BMI legt neuen Entwurf des IT SiG 2.0 vor", https://www.politik-kommunikation.de/gesetz-des-monats/naechster-versuch-bmi-legt-neuen-entwurf-des-it-sig-20-vor-1781324920#:~:text=W%C3%A4hrend%20die%20strafrechtlichen%20Vorschriften%20aus,Erh%C3%B6hung%20der%20m%C3%B6glichen%20Bu%C3%9Fgeldzahlungen%20vor, accessed Oct. 2020.

Wagener, T. (2020): „Low Economic Cost of Excluding Huawei and ZTE in European Markets," U.S. Department of State Office of the Chief Economist Working Paper, November.

Wang, Z. (2019): "Systematic Government Access to Private-Sector Data in China", https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-11, accessed Oct 2020.

Watts, J. (2019): "A framework for an open, trusted, and resilient 5G global telecommunications network", https://www.atlanticcouncil.org/in-depth-research-reports/report/a-framework-for-an-open-trusted-and-resilient-5g-global-telecommunications-network/#stateofcompetitionandrisk, accessed Oct 2020.

Washington Post (2019): "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible", https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html, accessed Nov. 2020.

Washington Post (2020): "Huawei tested AI software that could recognize Uighur minorities and alert police, report says". https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/ , accessed Dec. 2020.

Wheeler, T. and Simpson, D. (2019): "Why 5G requires new approaches to cybersecurity", https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/, accessed Oct 2020.

Williams, C. (2020): "Espionage and the race for a coronavirus vaccine", Canberra, https://www.canberratimes.com.au/story/6841183/espionage-and-the-race-for-a-covid-19-vaccine/, accessed Oct. 2020.

Winder, Davey (2019): Texas Cyber Attack has taken 23 Government Agencies Offline, in: Forbes, Aug. 19, 2019, https://www.forbes.com/sites/daveywinder/2019/08/19/texas-cyber-attack-has-taken-23-government-agencies-offline/?sh=7840aab32d65, accessed Oct. 2020.

World Bank (2020): "World Bank Open Data ". https://data.worldbank.org/ , accessed Dec. 2020.

World Economic Forum (2020): "The Impact of 5G: Creating New Value across Industries and Society", Switzerland, http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf , accessed Oct 2020.

World Justice Project (2020): "WJP Rule of Law Index 2020", https://worldjusticeproject.org/, accessed Oct. 2020.

Xi JinPing (2015): Ministry of Foreign Affairs of the People's Republic of China, Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference, December 16, 2015, available at http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.

ABOUT THE AUTHORS

Prof. Dr. Christian Dörr studied computer science and business administration at the University of Paderborn and has obtained a joint PhD in computer science and cognitive science from the University of Colorado at Boulder, USA. He is professor for cybersecurity and enterprise security at the Hasso-Plattner-Institute for Digital Engineering and the University of Potsdam. His core area of expertise is network and communication security, cyber threat intelligence and critical infrastructure protection.

Dr. Enrico Frumento is a Domain Specialist in the cybersecurity team at Cefriel a European and privately funded research and innovation project on ICT Security. He is the author of subject-related publications and books and 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.

Carlos Oliveira has an MScC in Software Engineering from the University of Coimbra, and is the Head of New Ventures for Ubiwhere, a company focused on Future Internet Technologies and Smart City platforms since its founding. Carlos has also worked as a Senior Product Manager in large-scale data-intensive consumer products where he has dealt with the practical implications of handling and securing large swathes of consumer information and has many years of expertise in R&D and commercial projects in the telecommunications sector.

Gianmarco Panza is a Senior Domain Specialist in the different fields of networking at Cefriel, a European and privately funded projectof R&D and innovations. He received a degree in Information Science Engineering at the University of Padova and a Master degree in ICT at Cefriel/Politecnico di Milan. 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 competences span from planning and design to testing and validation, as well as covering the novel services enabled by the next generation of networks, as 5G and beyond.

Stefan Rausch has an MA in political science and is a governmental relations specialist and project manager at the public affairs consultancy Rubis Development Group, focusing on defense, security and cyber-related topics. He has studied political science, communication and area studies in Rostock and Tallinn and worked at the Chair of Comparative Politics of the University of Rostock before joining Rubis DGroup in 2015.

Dr. Johannes P. Rieckmann studied economics and business studies in Bremen and Paris and holds a PhD. in development economics from University of Göttingen. He is senior research fellow at BIGS, and an alumni DAAD-AICGS research fellow.

Dr. Tim H. Stuchtey studied economics at the Westfälische Wilhelms-Universität Münster and has a PhD in economics from Technische Universität Berlin. He is the director of the Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS), a civil security think tank with a focus on economic aspects of security based in Potsdam. Tim is also a non-resident fellow at the American Institute for Contemporary German Studies (AICGS) in Washington, DC..

Dr. Reda Yaich is a senior researcher and cybersecurity team leader at IRT SystemX. Reda holds as PhD in Computer Science from the ENS Mines of Saint-Etienne with a focus on Trust Management using Artificial Intelligence technologies. He served as lecturer and/or research assistant in several universities (e.g. University of Saint-Etienne, University of Lyon) and engineering schools (ENS Mines Saint-Etienne, Telecom Bretagne, IMT Atlantique, ENSIBS, Telecom Sud-Paris). Reda has several publications in journals and conferences related to Decentralized Access Control, Authorization and Digital Trust Management.

IMPRINT

Located in Potsdam, the Brandenburg Institute for Society and Security is an independent, non-partisan, non-profit organization with an inter- and multidisciplinary approach with a mission to close the gap between academia and practice in civil security. The views expressed in this publication are those of the author(s) alone. They do not necessarily reflect the views of the Brandenburg Institute for Society and Security (BIGS).

Authors: Tim Stuchtey, Christian Dörr, Enrico Frumento, Carlos Oliveira, Gianmarco Panza, Stefan Rausch, Johannes Rieckmann, Reda Yaich

Title: The Hidden Costs of Untrusted Vendors in 5G Networks

Editor: Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH (Brandenburg Institute for Society and Security)

Dr. Tim H. Stuchtey
(responsible according to the German press law)

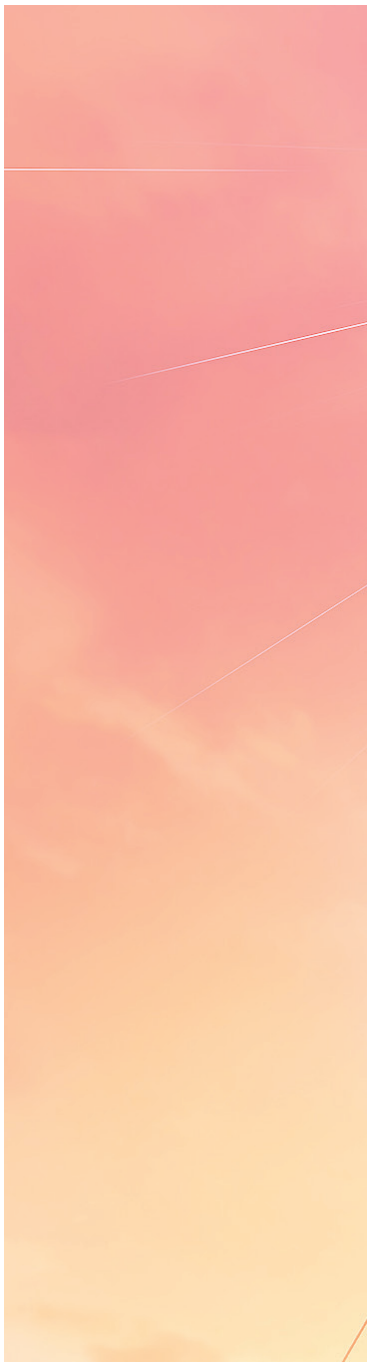
BIGS Policy Paper No. 8, December 2020

Frontcover: Sunshine Studio/Shutterstock.com

This publication was funded by a grant from the United States Department of State.

ISSN: 2194-2412

Brandenburg Institute for Society and Security
Executive Director: Dr. Tim H. Stuchtey
Dianastraße 46 . 14482 Potsdam
Tel.: +49-331-704406-0 . Fax: +49-331-704406-19
E-Mail: info@bigs-potsdam.org . www.bigs-potsdam.org



BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT