Fraunhofer

POSITION PAPER FROM THE FRAUNHOFER-GESELLSCHAFT

5G NETWORKS AND SECURITY

CONTENTS

1 EXECUTIVE SUMMARY

The rollout of 5G is set to bring new and innovative applications and business models. At present, only 5 percent or so of total data traffic is carried by mobile networks. In the future, however, 5G will set new standards. With its greater bandwidth, reduced energy requirements and enhanced capacity to connect devices and machines in real time, 5G will significantly increase the volume of data that is transmitted via mobile networks. Right now, 5G networks are being rolled out worldwide. The key drivers of innovation are 5G campus networks. These local 5G networks provide companies with opportunities to control their processes more efficiently.

The manufacturers of 5G network components occupy a key strategic position. This has led to the controversial situation in which network operators are now heavily dependent on the manufacturers of such components – not least Huawei. In turn, however, these manufacturers themselves are dependent on cutting-edge microelectronics, which only a few manufacturers – mainly in the USA – are able to produce. The key software for 5G networks is heavily protected by patents. This software is produced along a supply chain in which a large number of individual software components from diverse sources are combined to form a complex solution. To date, it has been very difficult to assign any backdoors – even when they have been detected – to specific authors.

In other words, the rollout of 5G will create multiple challenges and dependencies to which an adequate response is required. Particular attention should also be paid to terminal devices. In addition, it must be remembered that even conventional systems are open to considerable risks of state interference, not least for the purposes of espionage and sabotage. In the absence of suitable safeguards, this will apply even more so to 5G, especially given its wide range of potential applications and its possible use in safety-critical areas.

Fraunhofer makes eight recommendations that promise to bring greater security for 5G in the short and medium term and to increase technological sovereignty in the field of 5G in the long term. A ban on certain manufacturers, as currently being discussed, can help reduce risk, but it cannot completely eliminate it. Moreover, the resulting reduction in supply might also lead in the short and medium term to bottlenecks in the rollout of 5G and seriously impact Germany's competitiveness as a location for research and innovation.

Measures for immediate implementation (short/ medium-term perspective):

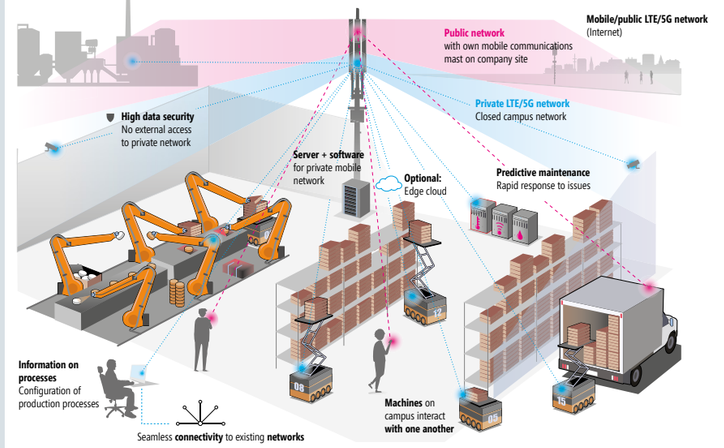
1. **Secure end-to-end encryption:** We recommend rapid and effective support for a blanket rollout of a public key infrastructure (PKI) for end-to-end encryption on the German and EU level.
2. **Rigorous testing and certification:** Authorities should establish appropriate test criteria and test procedures as soon as possible and progress with the establishment of test laboratories
3. **Creation of secure campus networks:** The state should provide support to German companies and startups that develop suitable solutions and thereby tap a growth market.
4. **Secure terminal devices:** The state should create incentives to promote greater security for terminal devices.
5. **EA European consortium to strengthen the market position of Nokia and Ericsson:** Europe should take swift action to avoid ceding control in this area..
6. **Using conventional networks for security-critical applications:** We recommend using only EU-sourced network components for applications with high security requirements

Stärkung der technologischen Souveränität (langfristige Perspektive):

1. **Developing 5G components in Europe:** We recommend implementation of a comprehensive research strategy for the development of 5G components. We estimate that the funding required for this will run into billions or even tens of billions of euros.
2. **Launching an open-source 5G partnership for Europe:** We recommend the development of a 5G reference platform and the establishment of communities to develop and operate open-source software for 5G.

Fraunhofer can substantially support all such measures in areas including the following:

- **Use of Fraunhofer test laboratories** to enable rapid formulation of test criteria and test procedures, and to establish dedicated 5G test labs and train technical staff.
- **Consultation in the creation and operation of 5G campus networks** based on our extensive experience working with living labs.
- **Securing 5G end-user systems** with, for example, Industrial Data Space (IDS) solutions.
- **Supporting the establishment of consortia** for the development of open interfaces and open reference architectures.



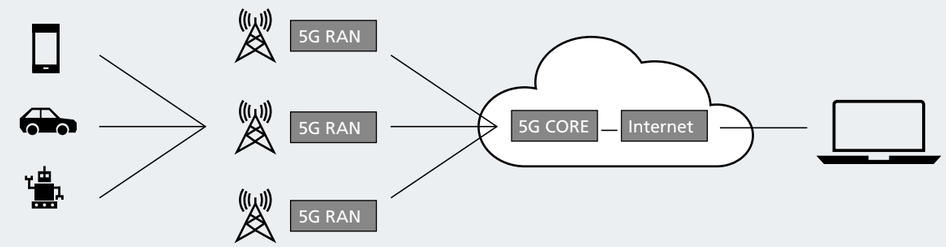
2 5G NETWORKS

A mobile communications network comprises three primary segments: terminal devices, the radio access network (RAN) and the core network (CN). The RAN comprises base stations with the corresponding antennas. The fourth generation of mobile communications technology (LTE) is largely used for the transmission of multimedia and other data content to and from terminal devices – as a rule, smartphones. On top of this, the 5G network will also bring a huge increase in new terminal devices. There will also be a paradigm shift in network architecture, which will make this architecture much more modular than is currently the case. This will offer greater flexibility in the creation of network infrastructure and make it possible, via software configuration, to equip this infrastructure for a wide variety of application scenarios.

A complex software architecture is used to realize the functionality of the core network, including gateways to other networks. Here, it must be remembered that by far the largest proportion of data traffic – currently 95 percent – is still transmitted via landline.1 However, this may significantly change in the next few years, once rollout of the 5G mobile network has been completed. It is therefore of vital importance at this early stage, during the actual planning and rollout phase, to exert a guiding influence on network development.

The 5G networks currently being rolled out in Germany are not being installed as standalone networks. Initially, the focus lies on upgrading existing 4G networks through the addition of 5G mobile radio components. What distinguishes 5G is its substantially increased software orientation and its use of visualization technology. The core network is composed of software modules and can be modified according to specific requirements (e.g., to support mobility, to ensure quality of service) and, if required, supplemented and enhanced with new software functions.

Schematic representation of a 5G network



1 https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2019/JB2018.pdf

Virtualization will reduce the proportion of specialized hardware that is currently required for digital signal processing in the RAN and for enabling network functions in the core network. This will enable software-based approaches on commercially available computer platforms. The division of the mobile radio network into centralized control units and distributed smart antenna units will also facilitate diversification among component suppliers. 5G technology supports applications with very different specifications. These range from multimedia applications, which require the transmission of large volumes of data, to IoT networks, which are connected to a larger number of terminal devices, and applications that require real-time data transmission. In other words, there will also be many different types of 5G network. By means of network slicing (through the provision of overlay networks), it will also be possible to provide very different services via one and the same physical network.

The performance characteristics of 5G mean that it will be able to efficiently support an extremely diverse range of applications for digital transformation. This means that there will be a dovetailing of 5G communications, data processing and application execution (sensor technology, actuator technology). For this reason, 5G terminal devices – in particular, machines, manned and unmanned vehicles, and IOT devices – will become extremely important. There will be a wide range of terminal devices, thereby enabling a diversification among users but also requiring for many terminal devices the implementation of individual security solutions to prevent eavesdropping – e.g., by means of secure end-to-end communication.

Another key innovation introduced by 5G will be the option to create either public or private 5G campus networks (Fig. 2). These networks will satisfy operators' needs for local data retention (data sovereignty), for wireless connectivity to company networks, and for real-time communications. These innovations will be enabled through the use of so-called small cells (low-powered radio cells densely deployed across a single location) and of dedicated, locally operated core networks. This will mean that companies can process their data directly in their own local data centers (edge cloud solutions) instead of transmitting this data via public mobile networks. Germany is regarded worldwide as a front-runner in the allocation of local 5G frequencies. As the first industrial type of 5G network, campus networks will therefore be required to demonstrate high standards of data security and reliability from an early stage onward.

To be able to identify the risks connected with the introduction of 5G, it is first necessary to understand the key dependencies and the possible dangers that these entail. In the following, we present the view of the Fraunhofer-Gesellschaft and then describe corresponding options and recommendations for action in order to reduce such risks. The recommendations of the Fraunhofer-Gesellschaft are to be seen as an addition to the EU report – the so-called 5G toolbox – published at the end of January 2020. This collates the results of a 2019 survey of EU member states and lists corresponding recommendations for measures to be taken to ensure the security of 5G networks.

2 *Infographic of a campus network ("Die Campus-Lösung," © Deutsche Telekom) https://www.telekom.com/de/konzern/details/ 5g-technologiein-campus-netzen-556690*

3 DEPENDENCIES

In order to arrive at a sound risk assessment, it is important to understand the complex dependencies that arise as a result of the specific characteristics of 5G infrastructure.

- **The technological dependency of network operators on component manufacturers while operating the network.** The market for 5G network components is currently dominated by three suppliers: Huawei, Ericsson and Nokia. In addition, ZTE and Samsung play an increasingly important role. Huawei and ZTE have a combined market share of approx. 40 percent; Nokia and Ericsson 31 percent. The rest of the market is controlled by specialized suppliers. Huawei has technological leadership in this sector and currently holds a dominant position in mobile network technology. The market for 5G modem chips, which is closely entwined with the market for 5G network components, is likewise controlled by a small number of suppliers: Qualcomm, HiSilicon (Huawei), Samsung, MediaTek, Sequans (at present only LTE) and, in the future, Apple (following its acquisition of the Intel modem business). Europe is relatively well represented in the sector for network infrastructure by Ericsson (Sweden) and Nokia (Finland). In the modem sector, however, European representation is rather weak (Sequans, France).

- **The technological dependency of component manufacturers** (routers, switches) **on their suppliers** (modem chipsets, transceivers)**.** All the leading manufacturers of network components are equally dependent on their product suppliers. At present, most of these are located in the USA, including the world market leaders for transceivers Lumentum and Finisar/II-VI. However, U.S. suppliers manufacture in China and Malaysia, which itself creates a supply chain dependency (see below). At present, Chinese manufacturers are exclusively active in the low-cost supplier segment. This in turn creates notable interdependencies between the U.S. supply industry, Chinese network component manufacturers, and network operators. In the light of recent media pronouncements by the U.S. government regarding the trustworthiness of Chinese manufacturers, it is highly likely that U.S. suppliers will cease manufacturing in China in the medium term.

- **The technological dependency of network operators and component manufacturers on the supply of complex software modules and software stacks for virtualization** – e.g., for network function virtualization (NFV) – and for software orientation – e.g., software-defined networking (SDN). This refers not only to manufacturers' proprietary software but also to an emerging trend towards open solutions with clearly specified interfaces for system components and their corresponding open-source reference implementation. Examples here include Telefonica's Open Source MANO (OSM) realization of ETSI NFV Management and Orchestration (MANO) software stacks and the Open RAN Alliance (http://www.oran.org) and corresponding open-source software stack for the radio access network (RAN). To date, however, these trends do not apply to the core network.

- **The technological dependency of all players on the entire hardware and software supply chain.** There are substantial dependencies on the hardware side alone, since network equipment providers depend on their mainly U.S. suppliers, and the suppliers themselves depend on their manufacturing locations, many of which are in China. In addition, there is also high dependency in the software supply chain, since complex software is made up of many software packages from different sources and also makes use of standard software components (e.g., software libraries).

- **The technological dependency on standard hardware technology** of fiber-connected cloud and edge cloud platforms. Here, the same dependencies exist as for all IT-based applications. While design and IP activities (e.g., Intel, AMD, ARM) are located in the USA or Europe, production takes place largely in Asia (Korea, Taiwan).

- **The technological dependency of new 5G networks on legacy systems,** i.e., 3G and 4G. Existing 4G networks will be supplemented with 5G mobile network components. In other words, the legacy 4G components will still be required.

- **The technological dependency of users** (industry, state, citizenry) on end-user systems.

- **Political dependency, resulting from state influence on national manufacturers by means of, for example, national legislation, which would have an indirect impact on Germany.** States can, for example, exert pressure on national manufacturers via legislation in order to facilitate or initiate opportunities for state-sponsored attacks and thus, in the technical sense, become attackers themselves. This concerns Huawei as well as many other manufacturers, including those whose components are to be found in the component lists of non-Chinese manufacturers.

4 RISKS

The dependencies outlined above pose immediate and significant risks for 5G networks. Of particular relevance are the intrinsic risks that can arise as a result of, on the one hand, technical weaknesses in the design and implementation of the 5G network and, on the other, the incorporation of built-in defects, whether intentional or involuntary. Given the new areas in which it will be used, 5G technology will also be open to a heightened risk of targeted attacks from outside.

In the following, we purposely exclude the risk of nonavailabilty. Generally speaking, the possibility of network failure cannot be eliminated. This applies to 5G and to other networks (e.g., in the energy sector or in relation to automotive applications). Any network must therefore take precautions against failure – by means of, for example, autonomous emergency control systems or redundancy in network design.

Biological risks arising from electromagnetic radiation are also purposely excluded from this position paper. Questions on this and related issues may be addressed to, for example, the Federal Office for Radiation Protection (BfS). In order to deal with such questions, the BfS is planning to establish a Competence Center for Electromagnetic Fields in Cottbus.

Nor does this paper address the current **patent situation and patent licensing policy** along with potentially emerging business models in, for example, the USA, since the impact of these is still highly speculative.

4.1 The manufacturer as risk factor

Manufacturers who knowingly equip their network components with corrupted hardware or software, and who thereby, for example, incorporate backdoors in the form of hardware or software Trojans – such manufacturers will then be able to tap data in the 5G core network, in the RAN and in terminal devices, and to carry out sabotage attacks. In the case of 5G, data will be encrypted before transmission via the mobile network and before transmission between network operators for roaming purposes. In the various components of the core network, however, data is processed unencrypted.

Using current methods, it is already possible to carry out a highly detailed investigation of hardware components and supplier components in order to determine whether they have hidden functionality or potential vulnerabilities. Similarly, today's methods already enable in-depth analysis and testing of software, especially when the source code is surrendered.

In the case of complex (software-based) systems, however, the use of static, one-off tests cannot eliminate the possibility of backdoors and malicious code to an acceptable degree. This applies to all products and all manufacturers. It is therefore essential that all components used in critical network areas, irrespective of their manufacturer, are tested and analyzed continually and systematically.

4.2 Software as risk factor

Software plays an important role in 5G architecture. For this reason, the risks that can be posed by software are substantial. In the past, software vulnerabilities were the **primary target**

for cyberattacks. Given that virtually all large software systems have such vulnerabilities, we can assume that this will be true of complex 5G software architecture. And since software modules get swapped, updated or patched in the course of their operative life, we also need – in addition to the systematic and rigorous tests referred to above – close inspection and monitoring over **the entire software lifecycle**.

4.3 The supply chain as risk factor

As described above, substantial dependencies exist within what is a highly specialized and globally distributed supply chain. In combination with a low level of diversification, this is a further source of substantial risk. In today's industry, complex software is no longer developed by one provider. Instead, it is made up a host of individual software packages and software libraries that comprise the software supply chain. Given these dependencies within the supply chain, it is practically impossible at present to attribute an identified vulnerability or backdoor to a specific supplier. For this reason, the regulations governing liability currently under discussion are likely to miss the mark. According to these regulations, manufacturers shown to have installed backdoors would be liable to fines of a severity likely to threaten their commercial viability – e.g., the equivalent of their annual sales.

4.4 The campus network as risk factor

Campus networks for supply infrastructures such as municipal utilities or connected industrial plants can be provided by network operators or built privately. Poor configuration, a lack of diversification in the technologies used, a failure to conduct security evaluations of the software used, and the inadequate implementation of access controls can all offer considerable scope for targeted attacks – including by organized crime. This in turn can massively compromise the security of supply or lead to significant damage as a result of espionage and sabotage.

4.5 The terminal device as risk factor

The terminal devices used in 5G applications often form part of a critical process or infrastructure. Examples here include machines in a production line and autonomous vehicles. Unlike the situation for core network components, there is a diverse range of components available for terminal devices. For this reason, the remarks concerning software-related risks also apply to terminal devices. Data can be encrypted end-to-end at terminal devices before transfer via the 5G network, thereby ensuring that it is securely transmitted throughout the entire 5G network, including any insecure components. However, the installation of spy software in terminal devices can be used to defeat end-to-end encryption, meaning that data can be tapped or modified at the source or at the destination. However, there already exists a host of solutions for securing terminal devices.

4.6 State interference as risk factor

In conventional systems, the risk of state interference – for the purposes of espionage or sabotage – is already substantial. Given the lack of diversification and the greater software orientation of 5G technology, both of which increase the scope for such interference, the risk is even higher in the case of 5G networks. State interference via domestic manufacturers, as is suspected in the case of Huawei, is just one example of this type of risk. Further examples of deliberate interference include the targeted infiltration of networks with manipulated software modules that can be run on any manufacturer's components, or with supplier technology upon which all manufacturers rely. The resulting damage depends on the kind of tasks that the manipulated components are required to perform in a network. Risk-exposed components should therefore only be used in areas in which an attack executed via them will remain largely without impact. Unfortunately, it is not always possible to harden networks by isolating such components in this way.

Excluding a manufacturer such as Huawei from the market would reduce the risk of state interference but not eliminate it completely. This would require the exclusion of all technology used in key areas and originating in countries that are suspected of exercising state interference now or in the near future. Moreover, this argument could be equally applied to 3G and 4G networks and to the landline network. At present, there are only three relevant suppliers of the elements for the 5G core network: Huawei (China) and Ericsson and Nokia (Europe). In addition, there is a string of smaller suppliers such as Mavenir, NEC, Samsung, Athonet and Qortus. However, none of these yet has competitive products on the market for equipping large networks. **Limiting sources of supply by excluding individual manufacturers might lead in the short and medium term to bottlenecks or delays in the rollout of 5G.**

5 OPTIONS AND RECOMMENDATIONS FOR ACTION

The risks described in §4 can be substantially reduced over the short to medium term through the implementation of a variety of individual measures or, even better, a bundle of measures. For example, end-to-end encryption and deep-dive security checks can significantly help to reduce the risk of espionage posed by component manufacturers, by outsourced components in the supply chain, and by state interference. In addition, state support for the creation of secure campus networks and networks with very high security specifications will help further reduce the risk posed by manufacturers and state interference. Systematic support for European technology can help counteract the high level of dependency on dominant manufacturers. In order to bring about a significant and lasting reduction of all the risks listed in §4, we recommend substantial state investment in research and development for 5G components, including all the requisite software.

5.1 Measures for immediate implementation (short to medium term)

A large proportion of potential espionage attacks can be averted by the implementation of secure end-to-end encryption. This ensures there is no sensitive plaintext data in the 5G network and that therefore this data cannot be directly tapped by any network component. Due to the lack of infrastructure, however, end-to-end encryption on a blanket scale is not an immediate option in Germany. In practice, the identification (and registration) of users and the secure distribution of public key certificates for large and comparatively open systems would still pose a major challenge. For this reason, there is still no blanket and widely used public key infrastructure (PKI) in Germany. Within a closed system, such as a network for the workforce of the Fraunhofer-Gesellschaft or other larger organizations, implementation of a PKI is technically feasible and is already being done. **We recommend blanket creation of a public key infrastructure. On this basis, it would also be possible to implement end-to-end encryption unilaterally on the German or EU level.**

Effective encryption presupposes that terminal devices are themselves secure. There is already a host of ready-to-use solutions available for securing end devices, most of which are marketed by SMEs. **The state should create incentives to promote greater security for terminal devices. This would represent an important and swiftly practicable step towards reducing attacks.**

End-to-end encryption alone does not suffice to eliminate the risk of damage through sabotage. However, **rigorous certification and testing** of software and hardware can play a big role in establishing confidence. This certification must serve to demonstrate the security of products and manufacturing processes. This in turn presupposes an independent security analysis conducted by a trustworthy laboratory. Ideally, the manufacturer will provide the lab with all relevant information (e.g., source code, design decisions). There are, however, limits to the testing of hardware and software, such that a residual risk always remains. Nonetheless, certification can help reveal gross design faults and eliminate numerous vulnerabilities in implementation. In the case of small systems or subsystems, certification can even make use of formal methods of validation and verification. It should also be remembered that software is sometimes modified after commissioning – by means of, for example, updates or patches provided by the manufacturer to remedy errors and the like. Therefore, each software update must be followed up by renewed security evaluation and certification. This is feasible but, in practice, extremely costly. Furthermore, the resulting delay in installing updates can easily lead to a reduction in security, since detected vulnerabilities remain unpatched until checks have been completed. **State authorities should therefore make it a priority to establish appropriate test criteria and test procedures and develop automated test tools. Work to accelerate the establishment and expansion of competent test laboratories with the requisite equipment should also begin immediately.**

This analysis of dependencies and risks clearly shows that for security-critical applications there is a need for alternative, highly secure networks – if required, based exclusively on conventional fiber and radio technology – or even for special, dedicated networks, as used by government agencies.

For applications with high security requirements, we recommend using only network components that originate in the EU. This does not, however, fully eliminate the dependencies that exist within the supply chain. It is therefore essential that hardware and software components are continually evaluated and tested throughout their entire life cycle.

We recommend the creation of secure campus networks. This will provide a good opportunity to harness the benefits of 5G technology for industrial applications in a secure and controlled environment. The state should specifically support the creation of such networks by assisting companies that supply technology developed for this purpose.

This can provide a major incentive for German or European start-ups to develop innovative solutions and gain a foothold in this growth market. At present, Nokia and Ericsson have a combined market share of only around 31 percent. By contrast, Chinese suppliers enjoy the immense advantage of a huge domestic market, which is essential for infrastructure providers. China has been an early adopter of 5G. In 2019, a total of 130,000 radio masts were converted from 4G to 5G at a cost of approx. 500 million U.S. dollars. The production of 5G modem chipsets using the 7 nm process is extremely expensive, involving one-off costs running into billions of euros. For this reason, market volume is much more important for 5G than in the case of 3G or 4G. At present, there are signs that the USA is considering acquisition of a controlling interest in Nokia or Ericsson. Europe should move quickly to prevent this and thereby ensure that control does not land completely in the hands of non-European countries.

We therefore recommend measures to substantially strengthen the market position of Nokia and Ericsson.

5.2 Strengthening technological sovereignty (long term)

In order to counteract the risks arising from a dependency on non-EU manufacturers and suppliers, we recommend **substantial state funding (on the EU level) for research and development of 5G components** (which will then be as independent as possible from non-EU suppliers). This is already practiced in a number of critical areas such as aerospace and defense technology in order to achieve independence in areas of technology that are subject to U.S. American ITAR restrictions. We estimate that the costs of developing alternative hardware components will be in the low tens of billions of U.S. dollars. For example, it would require various chips produced

using the 7 nm process.1 It would cost around 10 billion U.S. dollars to build a factory for 7 nm production in Europe.2 Here, we assume a development time of around five years.

It is possible to make up for lost ground in this area of technology – given sufficient political will and the requisite funding.

Furthermore, such a measure would create an opportunity for European companies and research institutions to incorporate their own intellectual property in present and forthcoming standards for future mobile communications systems. IP licensing costs account for around 15–20 percent of the cost of manufacture of a smartphone. In other words, even given the technological dominance of non-EU market players, this would still create a significant source of value for Germany and Europe. **In addition, substantial funding will be required for the introduction of these new technologies.** The UK telecommunications company Vodafone3 currently predicts costs of around 200 million euros for the planned swap of Nokia for Huawei hardware along with a possible delay in 5G rollout of between two and five years.

In addition to implementing controls on hardware development (including the controlled manufacture of all supplier components), it is only **logical that full controls should cover the software stack as well.** In the USA, the companies Dell, Microsoft and AT&T are now considering joint development of a common 5G software standard for telecommunication networks, which would run on standard hardware.4 However, it is by no means clear that this will come to fruition, not least because Huawei owns a large share of the IP and such a product would therefore (according to Huawei) remain one to two years behind comparable Huawei products.

In order to create alternatives to existing software stacks or those under development, we would recommend **support for open interfaces** – the Open API Initiative. This enables enhanced interchangeability of software components. Furthermore, we also recommend the launch of an **open 5G partnership for Europe**, in which European companies (users, operators, integrators, manufacturers) can define a 5G reference platform on the basis of available standards and best practice. In addition, we also recommend the establishment of **communities made up of broadly based industrial consortia to develop and operate open-source software**. This would offer a way of significantly reducing dependency on individual suppliers. Joint development in an open environment will also provide the requisite transparency and ensure that this enormous development effort can be met. Moreover, there will be attractive opportunities for startups and SMEs to contribute to an open 5G ecosystem.

5.3 Potential Fraunhofer contributions

Fraunhofer has considerable expertise in both software and hardware as well as hardware security labs with the very latest in measurement equipment and analysis methods.

As a neutral partner to German and European industry, with extensive know-how and first-rate lab facilities, Fraunhofer is an ideal source of expert consultation and support for government policy.

Fraunhofer offers its collaboration to government and industry in the following areas:

- **Creating additional labs to conduct analyses**
- **Training specialized staff**
- **Developing test criteria and test procedures**
- **Creating security solutions for terminal devices (trusted connector technology from the International Data Spaces Association) and other developments**
- **Further developments for radio access networks and core networks**
- **Consultation, planning, rollout and operation of secure 5G campus networks**

1 https://semiengineering.com/big-trouble-at-3nm/: "Generally, IC design costs have jumped…to $297.8 million for a 7nm chip"

2 https://venturebeat.com/2018/08/28/why-the-10-billion-chip-factory-club-just-got-smaller/

3 See https://www.heise.de/newsticker/meldung/Vodafone-Austausch-von-Huawei-kostet-Millionen-4655846.html; February 7, 2020

4 https://windowsunited.de/huawei-usa-planen-alternative-5g-software/; February 5, 2020

Editorial notes

Published by
Fraunhofer-Gesellschaft e.V.
Hansastrasse 27c
80686 Munich, Germany

Editorial team
Roman Möhlmann, Fraunhofer-Gesellschaft e.V.
Dr. Beate Rauscher, Fraunhofer-Gesellschaft e.V.
Dr. Jan Weber, Fraunhofer-Gesellschaft e.V.

Authors
Prof. Dr. Claudia Eckert, Fraunhofer AISEC
Prof. Dr. Thomas Magedanz, Fraunhofer FOKUS
Prof. Dr. Manfred Hauswirth, Fraunhofer FOKUS
Prof. Dr. Martin Schell, Fraunhofer HHI
Prof. Dr. Albert Heuberger, Fraunhofer IIS
Bernhard Niemann, Fraunhofer IIS
Dr. Haya Shulman, Fraunhofer SIT
Prof. Dr. Michael Waidner, Fraunhofer SIT

Photo acknowledgments
Page 5: Fraunhofer IPA / Rainer Bez
Page 7: Die Campus-Lösung / Deutsche Telekom
All other photos: iStock

Design
Ariane Lange, Fraunhofer-Gesellschaft e.V.