hgi
Horst Görtz Institute
for IT Security

Whitepaper – 5G

What does the "fifth generation" of the new mobile phone standard mean for IT security?

Introduction

5G – the "fifth generation" of mobile Internet and communications – will be available in Germany from 2020. Unlike the predecessor 4G, this does not only refer to the radio standard (LTE); 5G rather covers the entire network infrastructure and includes various communication technologies. So the term becomes synonymous with the complete interconnection of economy and society with the Internet. The real-time data transmission and enormous network capacities enable numerous applications such as in production, logistics, autonomous driving, smart cities or the Internet of Things, which so far have been unimaginable.

Germany would like to play a pioneering role internationally in 5G. In spring 2019 the Federal Network Agency granted licenses for a total of 6.55 billion Euros, as a basis for this expansion. The construction of the network begins now, but what exactly is 5G? Who is involved in this innovation? Which contribution can IT security research make to tackle the challenges 5G faces?

This white paper addresses these questions and argues that 5G is inseparably connected to IT security. If we want to take advantage of 5G in the future – no matter if private or industrial – security must not be marginally considered but has to play a central role.

In a nutshell: What is 5G?

Under the collective term 5G various key technologies are summarized. The access networks are the basis; the existing 4G/LTE networks will be merged with the 5G (*New Radio*) technology. The higher speed data transmission can thus achieve shorter latencies (*reaction times*).

In the second step, an "own" 5G core network will be implemented. In addition to mast and roof sites, small radio cells (*small cells*) and larger multi-antenna systems (MIMO – multiple Input, multiple output) are used and through *beamforming* – the variable and thus targeted alignment of signals to end devices – be rounded off.

Based on the access networks, the virtualization of networks form a new element of 5G. The local network is given a virtual layer and thus enables a location-independent control of services and the allocation of resources. An innovative element of 5G is its cloud base. Depending on the application, network operators can use slicing to provide their customers with various transmission rates and response times in "portions"; this enables greater efficiency and flexibility. In contrast to traditional data networks, this results in a close interaction between hardware and software, because configuration and commissioning is largely software-based. Only by combining the various solutions all the advantages of 5G will be fully exploited (see box).

!

The advantages of 5G at a glance

→ *Speed* – with data rates of up to 10,000 Mbit/s, 5G would be 100 times faster than 4G

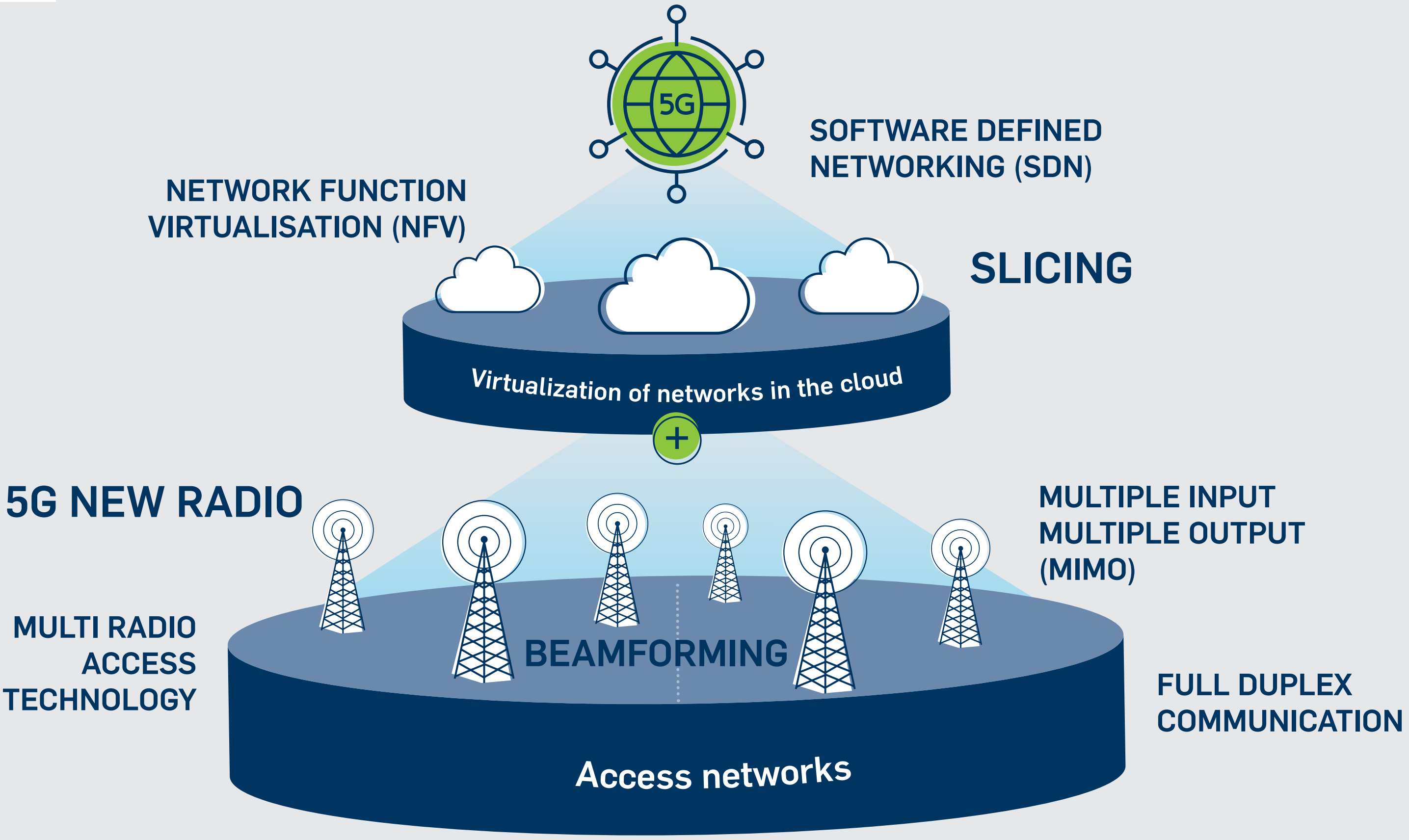
→ *Capacities* – the network capacities could increase LTE by 1,000 times

→ *Lower latency times,* i. e. the time span for an activity from one device to another. This could be in fractions of milliseconds, i. e. virtually take place in real time

→ A 90 % reduction in energy costs per mobile service in comparison with current consumption

?

What's 5G?


5G
SOFTWARE DEFINED NETWORKING (SDN)
NETWORK FUNCTION VIRTUALISATION (NFV)
SLICING
Virtualization of networks in the cloud
+
5G NEW RADIO
MULTIPLE INPUT MULTIPLE OUTPUT (MIMO)
MULTI RADIO ACCESS TECHNOLOGY
BEAMFORMING
FULL DUPLEX COMMUNICATION
Access networks

Glossary

→ *Full Duplex Communication* (full duplex) means simultaneous receiving and sending of information.

→ *MIMO – Multiple Input, multiple output* enables data streams to transmit and receive via several antennas simultaneously. This increases the transmission speed.

→ *Multi Radio Access Technology* (RAT) is a general term for the various physical connection methods for radio-based communication networks.

→ *Network Function Virtualisation* (NFV) comprises various cloud and virtualization technologies and enables the control of network functions via software.

→ *New Radio* is an umbrella term for the access technologies used in network roll-out for 5G and is also partly used as air interface.

→ *Software defined networking* decouples hardware and software in a network from each other and thus facilitates the administration of networks

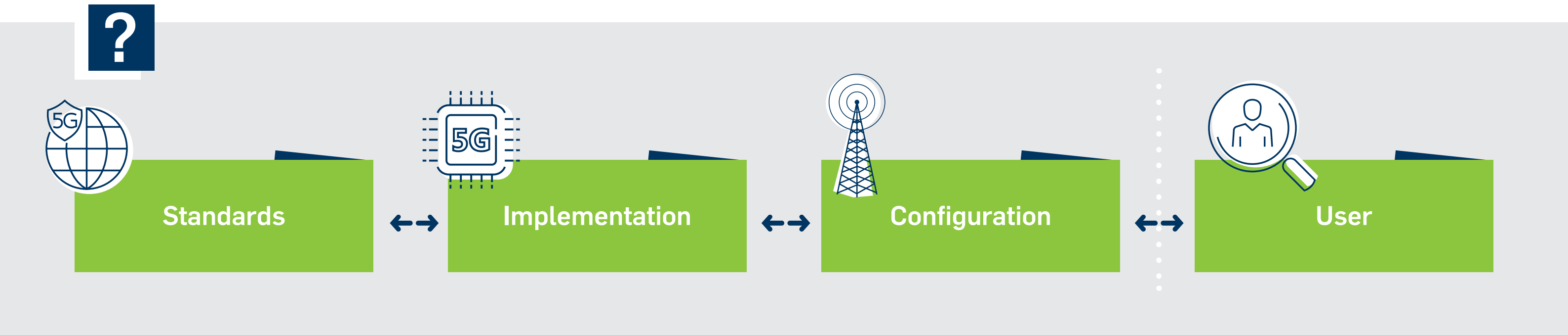
Not only the technical implementation of 5G is rather complex, but also the actors involved. In order to understand the requirements for IT security, one should not only look at the technical components, but also at the actors involved. Roughly four groups of actors involved in 5G can be identified:

First, the technical **standards** and specifications must be defined. The 3rd Generation Partnership Project (3GPP) is a worldwide cooperation of standardization bodies that pursues this goal and published the specifications with Release 15 and Release 16 in 2019. In 3GPP international mobile network operators, manufacturers, regulatory authorities, governments, stakeholders and umbrella organizations are involved.

During **implementation**, network operators will initially invest billions in new radio technology. However, there are only a few manufacturers that produce the 5G equipment. Many manufacturers buy 99% of the parts they process; this results in a very complex and fragmented supply chain. Manufacturers include Huawei, Ericson, Nokia, ZTE, Samsung and Qualcomm.

Once the access networks have been expanded, 5G network operation can begin. In the **configuration**, network operators must implement the technical standards and ensure smooth network operations. This includes not only the site maintenance but also the commissioning and control in the cloud. The relevant network operators in Germany are Deutsche Telekom, Vodafone, Telefonica and 1&1 Drill.

In the last step, the actual application of 5G takes place. This **operationalization** enables a multitude of application possibilities such as in industrial production and logistics, autonomous driving, medicine, smart cities and in general in the field of the internet of things. The users can be small and medium-sized companies, large corporations, start-ups, municipalities, but also private users.



What are the challenges for (IT) Security? What are relevant research questions for the future?

The security of mobile networks depends on the interaction of the different levels and is becoming more complex and thus more vulnerable to security gaps due to 5G in terms of the actors involved and the technical fragmentation.

The requirements for IT security are increasing as a result of 5G at all levels – starting with standardization, through implementation and configuration, to operationalization. In the public debate, however, there is a strong focus on implementation and the question of dependency on (mostly foreign) manufacturers. This debate on the "politicization of the supply chain" is justified, but falls too short: when it comes to the question of the security of systems and networks, the debate should not focus on individual manufacturers, but consider the interaction of the different actors equally. Thus, standardization and its implementation in configuration are just as relevant as risk minimization at operator level. Furthermore the orchestration of 5G networks via the cloud particularly strengthens the role of software (security).

The following showcase lists examples of challenges and research questions in the areas of **standardization, implementation** and **configuration** that are relevant from the perspective of the Horst Görtz Institute for IT Security. The list does not claim to be exhaustive, but is rather intended to increase awareness of the complexity of the topic. Overall, the introduction of *Cyber Physical Systems* (CPS) components – the connection of mechanical components with software – increases the sensitivity to external attacks. For companies it must therefore be ensured that intellectual property is protected in the best possible way. The fields of application of 5G are so diverse that even here it can only be suggested which challenges/questions are still unresolved. Like a red thread, the **human factor** plays a central role at all levels outlined above and should be considered in research with determination. Humans set the standards, act as developer, IT integrator or system administrator of technologies and security mechanisms, but also as users in the application. This raises the fundamental question: How can security mechanisms at all levels of the value chain be designed in such a way that they can be effectively applied to the relevant groups of users?

? Future research questions

Standards

Challenges

- → The multitude of actors involved (and interested parties?) in the negotiations (mostly) does not lead to anything but the smallest common consensus. For IT security this usually means cutbacks (e.g. the encryption of radio connections is still optional for this reason).
- → There is a conflict of interests between security requirements on the one hand (e.g. through end-to-end encryption) and lawful prosecution by police and justice on the other hand.

Still unresolved

- → How secure and robust are the 5G standards (3GPP) for various social use cases?
- → How can be ensured that the 5G standard intentional or unintentional contains no vulnerabilities?
- → How must the state design framework conditions to ensure that the security requirements are met?

↕

Implementation

Challenges

- → Interpretation of the complex standards is often ambiguous and leaves much room for interpretation.
- → The supply chain is complex and fragmented; this high interdependence makes trustworthiness along the entire supply chain difficult but mandatory.
- → *Pentests* or *security assessments* help, but it can never be proven beyond doubt that malicious software or back doors in networked systems exist.

Still unresolved

- → How can a manufacturer ensure that the supplied hardware or software doesn't contain vulnerabilities?
- → How can algorithms for encryption and integrity protection be implemented with high performance and still meet the data rates of 5G?
- → How can you test whether the equipment meets the standard at implementation and does not contain any intentional or unintentional errors?
- → The research must develop (standardized) procedures, which detects and prevents back doors.

↕

Configuration

Challenges

- → Interpretation of the complex standards during configuration is not definite and leaves much room for interpretation.
- → The operators are responsible for the control and data backup, which gives them a more important role regarding security functions than in the past.
- → Due to the new technologies, every manufacturer must constantly install software updates; the maintenance of the software requires the training of qualified employees.
- → In justice/criminal prosecution restrictions are feared, as e.g. IMSI (International Mobile Subscriber Identity) Catcher will be no help anymore for the police in the future. They can recognize, which mobile phones are at a certain point in time at a (crime) scene.

Still unresolved

- → How can security be provided given the complexity of networks and systems?
- → How do operators implement specific configurations of network equipment?
- → How can the permanent security of a complex system be ensured?
- → How much (IT) security is desired by the state?

↕

Users

Challenges

- → Increased digital networking increases the vulnerability of data and processes
- → The increased requirements for IT security not only must/can be covered on the operator side, but must also be integrated into internal processes and structures of the users.

Still unresolved

- → How can the confidentiality, integrity and availability of systems - whether embedded or software-based - be ensured?
- → How can "Security by Design" and "Privacy by Design" – the initial integration of security and privacy mechanisms in software components used – be effectively implemented in this dynamic environment?

Conclusion

5G enables speed, higher capacities and low latency times through a combination of various technologies, while at the same time reducing energy costs. Both the technical implementation and configuration as well as the actual fields of application are as exciting as they are forward-looking.

The expansion of 5G should be driven forward and is highly relevant for Germany's technological and economic development. It must be taken into account that 5G will simultaneously increase the vulnerability of the economy and society – regardless of which specific manufacturers, operators or users will ultimately be involved. The interplay between standardization, configuration and implementation must be carefully designed for the secure expansion and implementation of 5G, so that users can benefit from the positive effects of the technologies.

A political and social discourse on the question of how much (IT) security is desired in connection with 5G is still open. In June 2019, the Ministers of Justice of the Federal States presented a proposal for a resolution in which they point out the threat to surveillance capabilities for law enforcement in this context (e. g. restrictions are suspected due to end-to-end encryption or ineffectiveness of IMSI catchers, see "Research questions of the future"). This points out that the issue of 5G must not only be considered from a technical point of view, but should definitely be supplemented by legal and social science considerations.

In our view, IT security along the entire chain is a central precondition for the positive benefits of the new key technologies. For this reason, close cooperation between research, industry and politics is necessary to minimize risks and fully exploit potential. The research questions outlined above will be followed by numerous other essential questions. It is therefore absolutely necessary to accompany the new challenges in an iterative process involving all relevant actors and beeing supported by research.

!

About the HGI

The Horst Görtz Institute for IT Security (HGI), Research Department of the Ruhr-Universität Bochum (RUB), was founded in 2001 to address the Europe-wide deficits in IT security research. At the HGI, 26 professors and their working groups from the fields of electrical engineering and information technology, mathematics and computer science as well as humanities and social sciences are currently conducting research.

In this interdisciplinary environment, almost all aspects of IT security are covered. With around 200 scientists, it is one of the largest and most renowned higher education institutions in Europe in the area of IT security.

www.hgi.rub.de | www.casa.rub.de

Further information

→ On Security Research Towards Future Mobile Network Generations, David Rupprecht, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, Christina Pöpper, IEEE Communications Surveys and Tutorials, Volume: 20, Issue:3, 2018 hgi.

Do you have questions?

Ruhr-Universität Bochum | Horst Görtz Institute for IT Security
Universitätsstrasse 150 | Room ID 2/141 | 44780 Bochum

Friederike Schneider, M.A.
Head of Ressort Transfer, Research Department IT Security
T (+49) (0) 234 - 32 29975 | friederike.schneider@rub.de