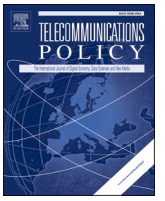
Telecommunications Policy 48 (2024) 102867

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol



Internet of Things, critical infrastructures, and the governance of cybersecurity in 5G network slicing

Günter Knieps

Institut für Wirtschaftswissenschaften, Albert-Ludwigs-Universität Freiburg, Abteilung für Wirtschaftspolitik, Insb. Wettbewerbsökonomie, Rempartstrasse 16, D-79085, Freiburg I.Br, Germany

ARTICLE INFO

JEL classification:
L96
L98
O33

Keywords:
5G network slicing
Cybersecurity
Critical infrastructures
Internet of Things
Virtual networks
General-purpose technologies

ABSTRACT

Over the last decade, cybersecurity has become a disruptive challenge driven by the shift to 5G networks. 5G is an application-agnostic general-purpose technology (GPT) characterized by its major role as multidimensional upstream technology for a large and open set of downstream Internet of Things (IoT) applications and use cases in various network industries and, more generally, within the economy as a whole. The focus of this paper is on the network economics of cybersecurity governance, considering the interplay between the recent EU cybersecurity regulatory framework, the extensive standardization efforts of international standardization organizations, and the economic incentives to tackle 5G network performance and security challenges. Based on the economic concept of 5G-based network slicing, the entrepreneurial challenges driven by the Internet of Things (IoT) are analyzed with an eye towards the complementarity between the physical side and virtual side of IoT applications. Network slicing gains particular relevance in the context of different types of logically separated, QoS-differentiated 5G bandwidth capacities, which are combined with other virtual resources such as sensor networks, data storage and processing, together with end-to-end slice security. It is shown in this paper that economic incentives for the implementation of 5G cybersecurity cannot be considered in isolation but must be viewed in combination with other performance requirements of 5G network slices. This is the driver for implementing network slicing architectures within 5G networks that feature a multitude of heterogeneous network slices with different QoS differentiation and various cybersecurity requirements.

1. Introduction

The debate surrounding security challenges in cyberspace and the many faces of potential cybercrime has a long tradition dating back to the origins of the public Internet. Research on cybersecurity is an interdisciplinary endeavor. The Internet Engineering Task Force (IETF) has undertaken substantial efforts to develop technical security standards for the Internet protocol with a particular focus on data transmission with tunneling and encryption mechanisms. However, active security management of the public Internet – for example, the introduction of an encryption layer or the introduction of access control mechanisms – was out of scope (Frankel & Krishnan, 2011; Kent & Seo, 2005; Clark, 2018, chapter 10, 189–226). There also exists a long tradition of dealing with the economics of cybersecurity by examining the incentives of various actors involved with the public Internet and how these affect their security decisions. Serious problems of cybersecurity within the public Internet have been identified, such as ongoing cybersecurity threats and

E-mail address: Guenter.Knieps@vwl.uni-freiburg.de.

https://doi.org/10.1016/j.telpol.2024.102867
Received 28 May 2024; Received in revised form 9 September 2024; Accepted 11 September 2024
Available online 18 September 2024
0308-5961/© 2024 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

associated blackmail and ransomware spread by botnets, large numbers of connected, infected computers responsible for malicious attacks or distributed denial-of-service attacks (Anderson, 2001; Anderson & Moore, 2006, ; Asghari, van Eeten, & Bauer, 2016; Van Eeten & Bauer, 2009). As long as the bulk of Internet traffic consisted only of e-mail or text files – types of traffic that generally have not been considered as highly critical – investments into cost-intensive encryption technologies or other security measures were not sufficiently incentivized for most Internet users and could also not necessarily be expected to result from competition among Internet Service Providers or other Internet intermediaries.

Since the pathbreaking work by Bresnahan and Trajtenberg (1995) the analytical concept of general-purpose technology (GPT) gains importance to characterize the pervasiveness and innovational complementarities of upstream technologies to stimulate innovations in a large and open set of downstream sectors. During the last decade, cybersecurity has become a disruptive challenge driven by the shift from 4G to 5G networks. Whereas fourth generation (4G) of mobile services mainly provide communication services, 5G networks offer a much broader range of broadband functionalities that enable the evolution of smart network industries. Due to fixed-mobile convergence and associated potentials of a large variety of QoS-differentiated broadband capacities, 5G networks function as an application-agnostic (upstream) multidimensional GPT – characterized by specifications of 5G frequency bands, throughput capacity and latency guarantees – providing a critical input for a large and open set of downstream Internet of Things (IoT) applications and use cases in various network industries and, more generally, within the economy as a whole. Depending on the different use cases QoS-differentiated broadband capacities are combined with complementary big data value chains enabling data generation, procession, storage and transmission to fulfill the required application-driven network performance and security (Heikkilä, Rissanen, & Ali-Vehmas, 2023; Knieps, Bauer, 2022; Magnaghi, Ghezzi, & Rangone, 2023, pp. 536–544; Parcu, Innocenti, Carozza, 2022). Problems of cybersecurity no longer challenge only broadband networks for communications and entertainment purposes, but also the resilience of application-based critical infrastructures and the security for a large variety of IoT applications (ENISA, 2019; ENISA, 2020). This is exactly why cybersecurity is gaining momentum as a subject of interest within the institutional reform process in the European Union and worldwide, with a particular focus on sectors of high criticality.

International standardization organizations are contributing to the development of relevant standards, with particular attention dedicated to 5G network performance and security challenges to fulfill the requirements of complementary physical infrastructures and use cases. Because the need to invest into cybersecurity becomes highly important for the society as a whole, understanding the heterogeneity of cybersecurity requirements and the need for application-driven, incentive-based decision-making by the actors involved has become an unavoidable necessity.

This paper is organized as follows: Section 2 is devoted to characterizing the topical 5G cybersecurity regulatory framework. The goal of the EU regulations is to enhance the resilience of critical infrastructures and essential services from the EU cross-border perspective (NIS Cooperation Group, 2019). ENISA (the European Union Agency for Cybersecurity) has the mandate to integrate the efforts of international standardization organizations when designing European cybersecurity certification schemes, considering the private actors involved.

Section 3 is devoted to international standards and entrepreneurial decision-making, with a particular focus on heterogenous network slicing performance and cybersecurity requirements. In order to analyze the entrepreneurial incentives for heterogeneous network slicing and heterogeneous cybersecurity requirements at first, a schematic illustration of the architecture of 5G-based network slicing is provided. As shown in section 3.1. different slice service types are standardized with a large scope of economically incentivized entrepreneurial flexibility, enabling a large variety of heterogeneous network slicing with associated network slicing security requirements. As it is elaborated in section 3.2. entrepreneurial decision-making regarding cybersecurity must consider the other virtual network components such as QoS-differentiated bandwidth capacities, sensor networks, geo-locational services and big data processing. The entrepreneurial governance challenge is based on the organization of the interaction between 5G network providers, 5G virtual network service providers, and the platform operators focusing on the provision of the physical network services.

Section 4 is devoted to the cross-network and cross-country perspective of network slicing to provide the required QoS network performance and heterogeneous cybersecurity guarantees. In order to satisfy the interoperability requirements of different network providers necessary to provide end-to-end network performance and the guarantee of end-to-end network slicing security, the focus is placed on the large entrepreneurial potentials of peering, roaming, and IPX network concepts. Section 5 summarizes the conclusions.

2. Cybersecurity regulations for critical infrastructures and essential services in the EU

The EU Reform process on cybersecurity regulations has gained momentum with the complementary character of recent cybersecurity regulations, enacting the Cybersecurity Act (Regulation (EU) 2019/881) of April 2019, regarding the upgraded mandate of ENISA (renamed to the European Union Agency for Cybersecurity), and on the Information and Communications Technology (ICT)

cybersecurity certification.[1] Furthermore, the Directive on the resilience of critical entities (Directive (EU) 2022/2557)[2] and the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)[3] have both been adopted by the European Parliament and the Council in December 2022.

A particular goal of the EU regulatory framework is to tackle the increasing cybersecurity challenges within 5G networks, focusing on the increasing interconnection and interdependency between physical and digital infrastructures with the goal of enhancing the resilience of critical infrastructures and essential services. The European Commission has the mandate to integrate the European and international standards and technical specifications and to interact with ENISA and the Cooperation Group (consisting of representatives of Member States, the Commission, and ENISA), considering the inputs of the private actors involved (NIS 2 Directive, (EU) 2022/2555, Articles 14, 20, 21).

The yearly ENISA Threat Landscape reports on cybersecurity within the EU have been issued since 2004 and have been addressing 5G networks since 2019, along with the concomitant increase of cybersecurity threats due the increasing complexity and scope of 5G-based IoT applications (ENISA, 2019; ENISA, 2020, ENISA, 2022, ENISA, 2023). The EU Toolbox of risk mitigating measures, along with its associated risk categories and scenarios, is of particular relevance, enabling the development and implementation of risk operation plans. The focus is on the important decision-making role of the relevant entrepreneurial actors involved within the cybersecurity value chain – particularly 5G network operators, equipment manufacturers, and cloud service providers – considering the international standards of 3GPP and other relevant standards committees (NIS Cooperation Group, 2020, pp. 5, 10; 2023; NIS 2 Directive, EU 2022/2555, Article 21; European Commission, 2019; European Commission, 2023a, European Commission, 2023b). Of particular relevance are the extensive standardization efforts of 3GPP and the security efforts of the mobile network operators and other stakeholders involved, such as cloud providers, equipment manufacturers, content providers, and end-users of 5G mobile networks (NIS Cooperation Group, 2020, p. 10; GSMA, 2023b, pp. 5–9). The goal is to improve the cyber resilience of public and private entities in specific sectors, establishing a non-exhaustive list of essential services in the sectors and subsectors with a particular emphasis on cybersecurity resilience as well as digital infrastructures and ICT services. Subsectors within the energy sector are electricity, district heating, oil, and gas; within the transport sector, subsectors are based on air, rail, water, and road transport. In addition, banking and financial markets, healthcare, and drinking and wastewater supply and distribution are listed. Among the large and ever-expanding scope of digital marketplace actors, one can include cloud computing services providers, data center service providers, trust service providers, and managed security service providers (NIS 2 Directive, (EU) 2022/2555, Article 3 and relevant sectors and subsectors referred to in Annex I and II).

3. Standard committees and entrepreneurial decision-making for heterogenous 5G network slices performance and cybersecurity

Due to the dynamic nature of 5G networks and the increasingly wide variety of 5G-based applications and use cases, heterogeneous cybersecurity requirements have evolved. Tackling cybersecurity threats has become an ongoing technological race and it cannot be expected that all cybersecurity threats will ever disappear or can be avoided entirely. Instead, a pivotal challenge is to exploit efficient and differentiated governance incentives for the design of resilient 5G networks, as well as heterogeneous security requirements for a large and growing variety of application-driven downstream use cases. Since 5G networks have the character of application-agnostic general-purpose technologies, the resilience of 5G networks is necessary but not sufficient; in addition, end-to-end security must be guaranteed.

3.1. International standardization of network slicing types

The starting point is to exploit an inherent feature of 5G networks – network slicing into logically separated bandwidth capacities – to guarantee network performance as well as heterogeneous network cybersecurity requirements. Various standardization institutions are involved with several increasingly complex and ever-expanding standardization areas with growing cross-border relevance: Telecommunication Standardization Sector of ITU (ITU-T), 3rd Generation Partnership Project (3 GPP), Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), and the Global Systems for Mobile Communications Association (GSMA). Within the standardization procedures of the various standardization committees different slice service types are distinguished with a large scope of entrepreneurial flexibility, enabling a large variety of heterogeneous network slices – depending on the heterogeneous performance requirements for the IoT applications – and services with associated requirements to implement different network slices for safety-relevant and non-safety-relevant use cases and applications. Based on the IMT (International Mobile Telecommunications) “triangle” of combining three fundamental characteristics of 5G networks: throughput capacity, latency

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151/15, 7.6.2019.

[2] Directive (EU) 2022/2557 of the European Parliament and of the Council of 8 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333/164, 27.12.2022.

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, (NIS 2 Directive) OJ L 333/80, 27.12. 2022.

guarantees, and number of connections – which also may be combined, depending on the IoT requirements – the standardization process of network slicing has gained momentum (ITU-R, 2015; ITU-T, 2018; ETSI TS 123 501, 2020).

Network slicing standardization efforts tackle the increasing challenges in 5G networks with a particular emphasis on heterogeneous network security requirements (ITU-T, 2018, p. 10). A hierarchy of network slices can be implemented enabling the priority of a given network slice relative to others in order to fulfill service-specific QoS requirements and provide service-specific security (ITU-T, 2018 p. 10; GSMA, 2021a, p. 26). Standardization of network slicing architectures and concomitant 5G slicing types enable sufficient flexibility for the entrepreneurial design of network slices depending on the IoT use case requirements. Entrepreneurial security management considers the heterogeneity of security requirements in different network slices. With regard to the 5G standards, 3GPP addresses increasing security demands by introducing new security controls and secure inter-operation-enabling security at the network edge, secure communication, key management, and protection policy exchange. Depending on the requirements of the physical applications, the provision of network slices depends on heterogeneous virtual network resources, such as radio access technology, traffic bandwidth capacity, end-to-end latency, reliability, QoS guarantees of bandwidth and security measures to enable the required network performance and heterogeneous security levels. Different service types need different combinations of network resources, such as traffic bandwidth requirements, coverage area requirements, degree of isolation requirements, end-to-end latency requirements, mobility requirements, priority requirements, service availability requirements, mission critical support, slice-specific authentication, and authorization, etc. (ETSI TS 128 530, 2018, p. 9–10; GSMA, 2021a, pp. 11–63).

Network slicing architectures require appropriate mechanisms to prevent unauthorized entities from accessing slice-specific configuration, management, or accounting user information. "Service-specific security" describes the potential performance and security requirements that IoT application providers (industry verticals) may place in their service-level agreements regarding the provision of network slices and differentiating between no isolation, physical isolation, or logical isolation, depending on heterogeneous security requirements. Of particular relevance are rules regarding how to ensure that resources from different slices not impact each other, preemption rules when resources are scarce, making efforts to improve end-to-end security architecture, and addressing the challenges to tackle the security requirements of interoperator network slices (GSMA, 2021b, pp. 12–19). The important role of heterogeneous 5G performance requirements, as well as the active management of cybersecurity risks, requires architectural innovations in 5G network slicing through the application of security-by-design principles that enable important classes of use cases, such as smart urban, regional, national and cross-border transportation and networked automated vehicle applications, as well as 5G-based Future Railway Mobile Communication Systems (ITF, 2023, pp. 42-55; 3 GPP TR 22.889, 2021, pp. 219–220, 232–234).

3.2. Market driven 5G based network slicing and heterogeneous cybersecurity requirements

An important and mandatory requirement for 5G networks is that their network architecture must enable 5G network slices based on the virtual (logistic) independence of the bandwidth requirements. The role of entrepreneurial flexibility and competence within the 3GPP/ETSI/GSMA standardization procedures shifts the focus to the market-driven flexibility to apply 5G network slicing taking into consideration heterogeneous 5G performance requirements as well as heterogeneous network security requirements for a large variety of IoT applications entailing 5G-based critical infrastructures and network services from an end-to-end perspective.

A large variety of use cases may evolve based on an open set of heterogeneous 5G network slices, reflecting not only the technological but also entrepreneurial potentials on the virtual side for the provision of smart infrastructure networks and smart network services on the physical side. Future market developments are based on entrepreneurial decision making, with particular potentials for a variety of use cases such as industry 4.0, transportation and logistics (5G PPP Technology Board & 5G IA Verticals Task Force, 2020; 5G PPP, 2022; 5G PPP, 2024). 5G gains the role of a "game changer" for the innovative development of smart networks and innovative use cases with particular relevance for 5G-based local industrial networks (Knieps and Bauer, 2022). 5G networks offer a broad range of broadband functionalities that enable application-driven virtual networks for differentiated use cases combining QoS-differentiated bandwidth with other ICT components, such as sensor based big data collection and processing, location-positioning services, cloud computing, and edge cloud services. QoS dimensions offered by 5G in combination with edge cloud data processing enlarge the innovation opportunities for a large variety of use cases depending on requirements of tactile applications with very low latencies and very high reliability for data transmission. Examples are including advanced augmented reality (AR) and virtual reality (VR) for networked vehicle projects, smart city planning projects and 5G-based local platforms for smart manufacturing and smart ports.

In order to analyze the entrepreneurial incentives for heterogeneous network slicing and heterogeneous cybersecurity requirements at first, a schematic illustration of the architecture of 5G based network slicing is provided (see Fig. 1).

The entrepreneurial design of network slicing is driven by the economic concept of application-based virtual networks considering the opportunity costs of the different complementary virtual network resources bundled within the decision competence of virtual network providers (Knieps, 2017).[4] 5G-based heterogeneous network slices are featuring a multitude of QoS-differentiated bandwidth capacities together with complementary virtual network resources and heterogeneous cybersecurity measures to fulfil the requirements of a multitude of different physical IoT applications. Although there are many actors involved in providing the required virtual network resources based on the underlying 5G networks with independent property rights and decision competences, the

[4] Coase (1960, p. 43) underlines the importance of opportunity costs for economic decision making as follows: "Economists who study problems of the firm habitually use an opportunity cost approach and compare the receipts obtained from a given combination of factors with alternative business arrangements. It would seem desirable to use a similar approach when dealing with questions of economic policy and to compare the total product yielded by alternative social arrangements."

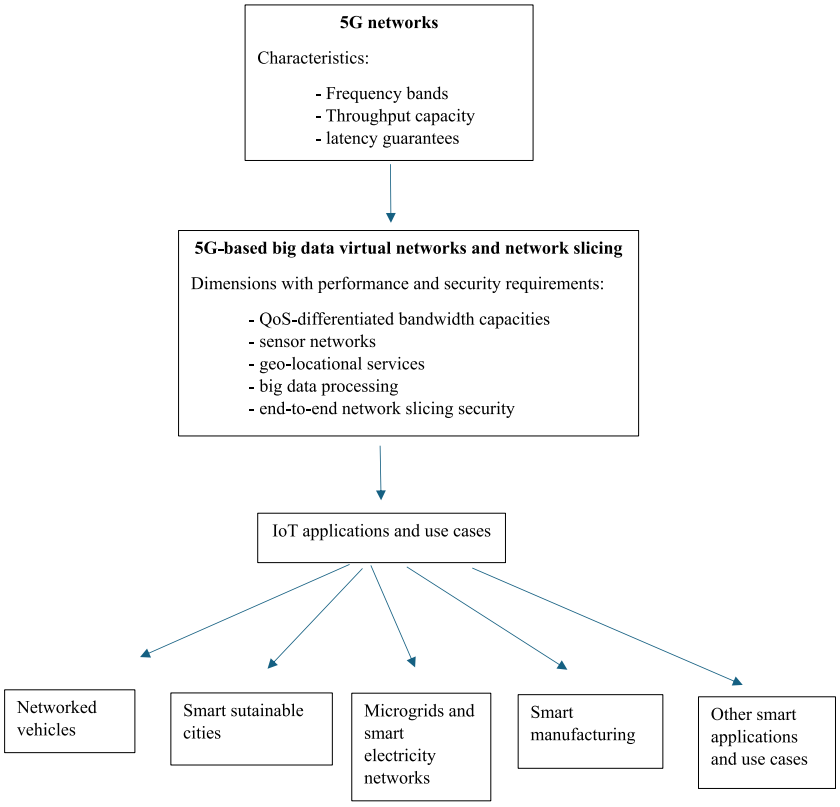


Fig. 1. The architecture of 5G-based network slicing.
Source: author

end-to-end organizational responsibility for network slices must be solely in the hands of the network slice provider based on a sequence of big data virtual networks (Knieps, 2022, pp. 299–302).

Entrepreneurial decision-making regarding cybersecurity must consider the other virtual dimensions of 5G big data virtual networks, such as QoS-differentiated bandwidth capacities, cloud computing, fog computing, and sensor components, that meet the requirements of the physical side of IoT applications. The entrepreneurial governance challenge is based on the organization of the interaction between 5G networks providers, 5G virtual network service providers, and the platform operators focusing on the provision of the physical network services. The design of network slicing based on the required sequence of 5G virtual networks is driven by the end-to-end requirements of IoT applications and concomitant requirements of 5G-based smart network infrastructures, with additional consideration given to the necessities of cybersecurity requirements.

Heterogeneous security requirements depend on the various requirements of the physical side. Based on the 5G triangle (ITU-R (2015, pp. 11–12), one can distinguish massive IoT networks slices with a large number of constraint devices characterized by low processing power and transmission capacities versus QoS guaranteed delay-sensitive tactile network slices.

The innovation potentials of network slicing range from the innovations of standardized slice service types to evolutionary dynamic slicing and Network Slice as a Service (GSMA, 2021b, pp. 41–42). Increased security problems may arise within the dynamics of network slicing. The focus on structural security governance problems depends on the design of network architectures and security by design principles, enabling active and potential competition among different players involved. Network slicing may evolve from "static" slicing within core networks introduced in 3GPP TS 23 501 release 15 (ETSI TS 123 501, 2018), with a few basic slice services types, towards dynamic network slicing innovations with cloud-native 5G core networks, programmable service-tailored radio access networks, transport network slicing, and further developments towards customized network slicing within Network Slice as a Service, which are enabling full automation in slice orchestration (GSMA, 2021b, pp. 41–43). High-level features, such as self-organizing networks for 5G networks and management data analytics for 5G networks, are evolving by utilizing the collection of network data to improve network slicing performance and service assurance (ETSI TS 128 530, 2023, p. 30).

Different actors may be involved in providing inputs in 5G network slicing, such as 5G network operators, communication service customers, communication service providers, network slice customers, and network slice providers. At the same time, different inputs can be provided simultaneously by the same actor (ETSI TS 128 530, 2018, pp. 16–17; GSMA, 2021a, pp. 9–11; GSMA, 2021b, pp. 11–12). Heterogeneous network slicing is not only based on heterogeneous QoS performance requirements, but simultaneously considers heterogeneous network security requirements, including security management and security procedures for network slices with a particular focus on network slice-specific authentication and authorization (ETSI TS 133 501, 2023, pp. 197–204). Generic

network slice attributes may include a large variety of different QoS performance characteristics – such as availability, area of service, delay tolerance, downlink throughput per network slice, and isolation level – but also include security aspects such as mission critical support and network slice-specific authentication and authorization (GSMA, 2021a, pp. 11–12, 26–28, 59–60).

The economic design of network slicing is based on entrepreneurial security and network performance decision-making and accounts for the opportunity costs of different complementary virtual network resources required. Under the responsibility of each network slice provider, different virtual network resources, such as bandwidth capacity, sensor networks, geolocation services, data processing and cloud computing, are combined simultaneously to fulfill the necessities of smart physical IoT applications, considering security and privacy requirements. The heterogeneous requirements of network slicing based on a sequences of virtual networks and concomitant cybersecurity needs make it necessary to implement 5G network architectures requiring incentive-compatible pricing, as well as investment decisions enabling hierarchies of classes of QoS-differentiated bandwidth capacities with stochastic and deterministic traffic classes and the concomitant requirements of market-driven network neutrality (Bauer & Knieps, 2018, p. 175; Knieps and Stocker, 2016, pp. 325–329; Stocker & Knieps, 2019, pp. 18–21).

4. The governance of cross-border 5G network slicing performance and security

The standardization process of network slicing remains an ongoing pursuit to realize cross-border, end-to-end network service and security requirements from IoT application providers along with the requirements of 5G network operators. The concept of 5G cross-border network slicing is strongly related to the connectivity and interoperability demands of 5G networks driven by the heterogeneous IoT downstream performance requirements and concomitant network slicing security. Interdomain end-to-end network slicing gains a particular challenge to tackle the increasing technical and governmental complexities due to the multitude of heterogeneous coverage domains of different network operators and associated decision competences. From the economic perspective of cross-border network slicing the quest arises, how to design and implement incentive-compatible solutions to establish the required interdomain end-to-end network slices which may either be based on combined horizontal sequences of intradomain network slices or alternative institutional arrangements. The increasing complexity of cross-border network slicing provides ample incentives for cooperation between different standardization committees.

To satisfy the interoperability requirements of different network service providers enabling end-to-end network slicing performance and to guarantee end-to-end network slicing security, the focus is to investigate the significant entrepreneurial potentials of cross-border peering and roaming while considering the role of IP packet eXchange (IPX) interconnection agreements (GSMA, 2021c). As it turns out IPX networks provide an important innovation for the interconnection among IoT based big data virtual networks and associated network slicing. Whereas peering has its origin in the direct connectivity between “neighboring” service providers with bilateral agreements to freely exchange their traffic, roaming provides the possibility for a network service provider to operate in a visited network. The goal of IPX networks is the exchange of IP-based services between customers of different mobile and fixed network operators, enabling interoperability between any type of service providers and supporting end-to-end QoS for roaming and peering (GSMA, 2009; GSMA, 2022a). IPX providers and Roaming Value-Added Services providers are important actors in the effort to enable reliable and secure QoS roaming services. A particular role of a roaming hub is to provide QoS-differentiated roaming services to 5G network operators without roaming agreements. The simultaneous determination of QoS guarantees and security guarantees depending on the IoT requirements is required to ensure the reliability and security of international roaming services (GSMA, 2022b, pp. 9–12).

If several 5G networks are involved, end-to-end network slicing requires incentive-compatible interconnection agreements between different 5G networks with the necessary prerequisites to exploit the governance potentials of peering, roaming, and IPX networks, together with 5G privacy and security policies. 5G network slicing – along with the potential of cross-border peering, roaming, and IPX interconnection agreements – has many facets. Of particular relevance is the cross-border perspective of network slicing in European 5G-based network industries to fulfill the heterogeneous end-to-end QoS network performance requirements and to provide the required heterogeneous end-to-end cybersecurity guarantees. Important classes of use cases are European highway systems, European energy networks, and European railway systems, entailing significant implications for cross-country network slicing performance and network slicing security.

5G European railroad systems, for example, are a particular relevant class of use cases illustrating the large potentials of heterogeneous network slices ranging from extreme security relevant network slices enabling train operator platforms shifting network intelligence from the railroad tracks to the trains and 5G-based train traffic control systems on one hand and 5G slices for communication and entertainment within the trains with lower security requirements on the other hand. Heterogeneous classes of use cases differentiate between safety-critical communication application-related use cases (such as railway emergency communication, automatic train protection support, monitoring and control of critical infrastructure related use cases, autonomous train control and operation), operation performance use cases (such as communication services between staff and passengers), and business use cases (such as applications to provide Internet services). Hence, heterogeneous classes of use cases may be provided within the Future Railway Mobile Communication System (FRMCS), with a particular focus on its roaming capabilities. It is of particular relevance for the operation of international trains (either for passengers or freight) that cross-border train operators can use a single FRMCS equipment together with slicing performance and security guarantees requiring the roaming of home network slices onto visited

FRMCS networks (3GPP TR 22.889, 2021, pp. 235–241).[5]

The necessity of implementing network slicing security arises irrespective whether interconnection agreements are based on peering or roaming with or without IPX network support. From the network performance perspective, incentives for heterogeneous network slicing require an incentive-compatible hierarchy of heterogeneous QoS bandwidth differentiation, together with other virtual network components. Based on the concept of 5G big data virtual networks, the governance of 5G network slicing simultaneously combines the requirements of cybersecurity and network slicing QoS performance to fulfill the cross-border requirements of smart networks.

A lean implementation of network slicing security requires that 5G network operators only reveal to an IPX network provider the network functions that are necessary for the implementation of interconnection agreements. Thus, a broad variety of heterogeneous cross-border, end-to-end network slices are enabled even if a large set of different 5G networks is involved. Depending on the use cases under consideration, network slices may be designed with specific roaming requirements. Technical and commercial agreements need to be tailored to implement 5G network slice roaming with a special emphasis on roaming security (GSMA, 2022a, pp. 26–28, 39).

5. Conclusions

The governance of network slicing is based on leveraging the concept of big data virtual networks and their problem-solving competence to combine the relevant virtual resources depending on the requirements of the IoT-driven physical side. The network economic incentivizing of cybersecurity cannot be considered in isolation but rather in combination with other dimensions of 5G virtual networks, such as 5G bandwidth capacities and latency guarantees combined with other virtual dimensions, such as data collection and data processing. The heterogeneous requirements of the virtual networks, along with concomitant cybersecurity requirements, lead to the problem-solving competence of hierarchies of QoS-differentiated bandwidth together with other virtual resources (sensor networks, data processing, etc.) and heterogeneous cybersecurity solutions, depending on the IoT requirements under consideration. This results in the implementation of network slicing architectures within 5G networks, featuring a multitude of heterogeneous network slices with varied QoS network performance and heterogeneous cybersecurity requirements.

The entrepreneurial governance problem in terms of guaranteeing network slicing security is based on a sequence of virtual networks, along with the role of the network slicing provider as network orchestrator, considering security requirements within the different dimensions of big data value chains (data collection, data processing, data aggregation, data transmission, etc.), and the interconnection between different virtual networks depending on the security requirements tailored for the needs of the physical applications. Of particular relevance are the cross-network and more general cross-country perspectives of network slicing to fulfill the required QoS network performance guarantees and the necessary heterogeneous cybersecurity guarantees from an end-to-end-perspective. Incentivizing cross-sector interconnection agreements are based on peering, roaming, and IPX agreements for end-to-end 5G network slicing performance and slicing security, as well as on the governance of 5G roaming security and IPX interconnection agreements.

CRediT authorship contribution statement

Günter Knieps: Writing – original draft.

Data availability

No data was used for the research described in the article.

Acknowledgements

Helpful comments and suggestions by Johannes Bauer and two anonymous referees are gratefully acknowledged. Many thanks go to Ryan Grabowski for his support in editing the final English version.

References

3 GPP TR 22.889, 2021 3 GPP TR 22.889. (2021). *3rd generation partnership project; technical specification Group services and system aspects; study on future railway mobile communication system; stage 1, V17.4.0.* Release 17.

5 G PPP, 2022 5 G PPP. (2022). Verticals cartography. https://standards-tracker.5g-ppp.eu/cartography.

5 G PPP, 2024 5 G PPP. (2024). *5G infrastructure public private partnership (PPP) programme, trials & pilots, summary brochure.* April, 5G-PPP.EU.

5 G PPP Technology Board & 5G IA Verticals Task Force, 2020 5 G PPP Technology Board & 5G IA Verticals Task Force. (2020). *Empowering vertical industries through 5G networks – current status and future trends.* Version 1.0, 20-08-2020.

Anderson, R. (2001). Why information security is hard - an economic perspective. *Seventeenth annual computer security applications conference*. New Orleans, LA, USA.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*, 610–613.

Asghari, H., van Eeten, M., & Bauer, J. M. (2016). Economics of cybersecurity. In J. M. Bauer, & M. Latzer (Eds.), *Handbook on the economics of the Internet* (pp. 262–287). Cheltenham et al: Edward Elgar.

Bauer, J. M., & Knieps, G. (2018). Complementary innovation and network neutrality. *Telecommunications Policy, 42*(2), 172–183.

[5] Different cross-border scenarios are explored within ETSI TR 103 459 (2020, pp. 40–49).

Bresnahan, T. F., & Trajtenberg, M. (1995). General purpose technologies: Engines of growth? *Journal of Econometrics, 65*, 83–108.
Clark, D. D. (2018). *Designing an Internet*. Cambridge, Massachusetts: MIT Press.
Coase, R. H. (1960). The problem of social cost. *The Journal of Law and Economics, 3*, 1–44.
ENISA. (2019). *ENISA Threat Landscape for 5G Networks, Threat assessment for the fifth generation of mobile telecommunication networks (5G)*. November: European Union Agency for Cybersecurity (ENISA).
ENISA. (2020). *ENISA Threat Landscape for 5G Networks, Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)*. December: European Union Agency for Cybersecurity (ENISA).
ENISA. (2022). *ENISA threat Landscape 2022, july 2021 to july 2022*. October: European Union Agency for Cybersecurity (ENISA).
ENISA. (2023). *ENISA threat Landscape 2023, July 2022 to June 2023*. October: European Union Agency for Cybersecurity (ENISA).
ETSI TS 123 501. (2018). *5G; system architecture for the 5G system (3GPP TS 23.501 version 15.3.0 release 15)*.
ETSI TS 123 501. (2020). *5G; system architecture for the 5G system (3GPP TS 23.501 version 16.6.0 release 16)*.
ETSI TS 133 501. (2023). *5G; Security architecture and procedures for 5G System (3GPP TS 33-501 version 17.10.0 Release 17*.
ETSI TS 128 530. (2018). *5G; Management and orchestration; Concepts, use cases and requirements, V.15.0.0, (3GPP TS 28* (p. 530). version 15.0.0 Release 15).
ETSI TS 128 530. (2023). *5G; Management and orchestration; Concepts, use cases and requirements, V. 16.6.0, (3GPP TS 28* (p. 530). version 16.6.0 Release 16).
ETSI TR 103 459. (2020). *Rail Telecommunications (RT); Future rail mobile communication system (FRMCS); study on system architecture, 1.2.1*.
European Commission. (2019). Twentieth progress report towards an effective and genuine security union, communication from the commission to the European parliament, the European Council and the Council. *Brussels*, 30.10. 2019, COM (2019) 552 final.
European Commission. (2023a). Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. *Strasbourg 18.4. 2023*. COM (2023) 209 final, 2023/0109 (COD),(proposed Cyber Solidarity Act 2023).
European Commission. (2023b). Implementation of the 5G cybersecurity Toolbox. *Brussels*, 15.6.2023, C (2023) 4049 final.
Frankel, S., & Krishnan, S. (2011). IP security (IPsec) and Internet key exchange (IKE) document roadmap. *RFC*, 6071.
GSMA. (2021a). Generic network slice template, version 5.0. *Official Document NG, 116*(1 June).
GSMA. (2021b). E2E network slicing architecture. *Version 1.0 , Official Document NG, 127*(3 June).
GSMA. (2021c). Guidelines for IPX provider networks (previously inter-service provider IP backbone guidelines). *Version 17.0, Official Document IR.34*, (18 May).
Heikkilä, J., Rissanen, J., & Ali-Vehmas, T. (2023). Coopetition, standardization and general purpose technologies: A framework and an application. *Telecommunications Policy, 47*. Article 102488.
ITF. (2023). Preparing infrastructure for automated vehicles. *ITF (international transport Forum) research report*. Paris: OECD Publishing.
ITU-R. (2015). *IMT Vision – framework and overall objectives of the future development of IMT for 2020 and beyond*. Recommendation ITU-R. M.2083-0.
ITU-T. (2018). *Requirements of the IMT-2020 network, Recommendation ITU-T Y.3101*.
Kent, S., & Seo, K. (2005). Security architecture for the Internet protocol. *RFC*, 4301.
Knieps, G. (2017). Internet of Things, future networks and the economics of virtual networks. *Competition and Regulation in Network Industries, 18*(3–4), 240–255.
Knieps, G. (2022). The economics of 5G-based network slicing in smart network industries. *Competition and Regulation in Network Industries, 23*(4), 296–310.
Knieps, G., & Bauer, J. M. (2022). Internet of things and the economics of 5G-based local industrial networks. *Telecommunications Policy, 46*(4), Article 102261. May 2022.
Knieps, G., & Stocker, V. (2016). Price and QoS differentiation in all-IP networks. *International Journal of Management and Network Economics, 3*(4), 317–335.
Magnaghi, M., Ghezzi, A., & Rangone, A. (2023). 5G is not just another G: A review of the managerial literature. *Proceedings of the 18th European conference on innovation and entrepreneurship*. ECIE.
NIS Cooperation Group. (2019). EU coordinated risk assessment of the cybersecurity of 5G networks. *Report*, 9 October.
NIS Cooperation Group. (2020). *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*. CG Publication 01/2020.
Parcu, P., Rossi, M., & Brennan, T. (2022). Innovation in 5G technology: Leadership, competition, and policy issues. *Telecommunications Police, 46*(4). Article 102277.
Stocker, V., & Knieps, G. (2019). Network neutrality through the lens of network economics. *Review of Network Economics, 17*(3), 115–150.
Van Eeten, M. J. G., & Bauer, J. M. (2009). Emerging threats to Internet security: Incentives, Externalities and policy implications. *Journal of Contingencies and Crisis Management, 17*(4), 221–232.