ETLA

Raportti | Report | 152

13.11.2024

5G in the Era of Geoeconomics: Playbook for Finland?

Petri Rouvinen, ETLA
Timo Ali-Vehmas, Aalto University
Timo Harakka, Parliament of Finland
Nina Hyvärinen, CKIR
Heli Koski, ETLA
Otto Kässi, ETLA
Ilkka Lakaniemi, CKIR
Denisa Mäki, CKIR
Kent Thorén, KTH

Suggested citation:
Rouvinen, Petri, Ali-Vehmas, Timo, Harakka, Timo, Hyvärinen, Nina, Koski, Heli, Kässi, Otto, Lakaniemi, Ilkka, Mäki, Denisa & Thorén, Kent (13.11.2024). "5G in the Era of Geoeconomics: Playbook for Finland?". ETLA Report No 152. https://pub.etla.fi/ETLA-Raportit-Reports-152.pdf

Abstract

As compared to the earlier generations of mobile communications (1G to 4G), the fifth one (5G) is a major business, regulatory, and technical discontinuity. Furthermore, unlike the previous generations, 5G is also much more of a geopolitical and geoeconomic battleground. These shifts are neither well-understood nor fully reflected in public and private strategies.

This report opens the Mobile is Global (MiG) project of CKIR and ETLA that is kindly supported by Business Finland. The project assesses geoeconomic realities influencing future developments in mobile communications, offers a roadmap to lessen future uncertainties, and provides recommendations for paths forward for Finnish and European policymakers and industry.

In this report, we give a specific interpretation of Finnish national interests in the context of 5G and use this interpretation to derive a framework to think about geopolitically motivate internal and external threats and security issues. We also discuss the broader context for thinking about the future of mobile communications and delve into its technical and regulatory aspects.

Tiivistelmä

5G geotalouden aikakaudella: Mikä on Suomen pelikirja?

Mobiiliviestinnän viidenteen sukupolveen (5G) liittyy liiketoiminnan, regulaation ja tekniikan näkökulmista huomattavia epäjatkuvuuksia aiempiin sukupolviin (1G–4G) verrattuna. Toisin kuin aiemmat sukupolvet, 5G on myös geopoliittinen ja geotaloudellinen taistelukenttä. Nämä epäjatkuvuudet ovat huonosti ymmärrettyjä, eikä niitä ole huomioitu riittävästi julkisen ja yksityisen sektorin strategioissa.

Tämä raportti aloittaa CKIR:n ja Etlan toteuttaman ja Business Finlandin tukeman Mobile is Global (MiG) projektin, jossa tutkitaan geotalouden vaikutuksia mobiiliviestinnän kehitykseen, laaditaan tiekarttaa tulevien epävarmuuksien vähentämiseksi sekä annetaan suosituksia suomalaisille ja eurooppalaisille päättäjille ja elinkeinoelämälle.

Tarjoamme tässä raportissa täsmennetyn tulkinnan Suomen kansalliselle edulle 5G:n kontekstissa ja luomme sen pohjalta viitekehyksen geopoliittisesti motivoituneiden sisäisten ja ulkoisten uhkien ajattelemiseksi. Käsittelemme myös mobiiliviestinnän tulevaisuuden laajempaa kontekstia sekä tarjoamme näkökulmia aihetta sivuaviin teknisiin ja regulatorisiin kysymyksiin.

PhD (Econ.) **Petri Rouvinen** on Elinkeinoelämän tutkimuslaitoksen tutkimusneuvonantaja ja Suomen itsenäisyyden juhlarahaston Sitran vanhempi neuvonantaja. (petri.rouvinen@etla.fi)

TkT **Timo Ali-Vehmas** on vieraileva tutkija Aalto-yliopistossa ja yksityinen sijoittaja. (timo.ali-vehmas@aalto.fi, timo.ali-vehmas@iki.fi)

Timo Harakka on kansanedustaja ja Helsingin yliopiston jatko-opiskelija. (timo.harakka@eduskunta.fi)

Nina Hyvärinen on Aalto-yliopiston kauppakorkeakoulun CKIR-yksikön vanhempi neuvonantaja ja NMH Global Oy:n toimitusjohtaja. (nina.hyvarinen@aalto.fi)

KTT **Heli Koski** on Elinkeinoelämän tutkimuslaitoksen tutkimusjohtaja. (heli.koski@etla.fi)

VTT **Otto Kässi** on Elinkeinoelämän tutkimuslaitoksen tutkija ja Research Associate Oxfordin yliopiston Oxford Internet Institutessa. (otto.kassi@etla.fi)

Tutkimusjohtaja **Ilkka Lakaniemi** on Aalto-yliopiston kauppakorkeakoulun CKIR-yksikön johtaja. (ilkka.lakaniemi@aalto.fi)

Denisa Mäki on Aalto-yliopiston kauppakorkeakoulun CKIR-yksikön tutkija. (denisa.maki@aalto.fi)

TkT **Kent Thorén** on Tukholmassa sijaitsevan KTH:n, Kungliga Tekniska högskolanin, liitännäistutkija ja Audax Strategic Advisorsin toimitusjohtaja. (kthoren@kth.se)

PhD (Econ.) **Petri Rouvinen** is a Research Advisor at Etla Economic Research and a Senior Advisor at The Finnish Innovation Fund Sitra. (petri.rouvinen@etla.fi)

DSc (Tech.) **Timo Ali-Vehmas** is a Visitor at Aalto University and Private investor. (timo.ali-vehmas@aalto.fi, timo.ali-vehmas@iki.fi)

Timo Harakka is Member of Parliament of Finland and PhD student at University of Helsinki. (timo.harakka@eduskunta.fi)

Nina Hyvärinen is a Senior Advisor at CKIR, Aalto University School of Business, and the CEO of NMH Global Oy. (nina.hyvarinen@aalto.fi)

Ph.D. (Econ.) **Heli Koski** is a Research Director at Etla Economic Research. (heli.koski@etla.fi)

DrSocSc (Econ.) **Otto Kässi** is a Researcher at Etla Economic Research and a Research Associate at the Oxford Internet Institute (University of Oxford). (otto.kassi@etla.fi)

Research Director **Ilkka Lakaniemi** is Director at CKIR, Aalto University School of Business. (ilkka.lakaniemi@aalto.fi)

Denisa Mäki is a Researcher at CKIR, Aalto University School of Business. (denisa.maki@aalto.fi)

DSc (Tech.) **Kent Thorén** is an Affiliate Researcher at KTH, the Royal Institute of Technology (Stockholm), and the CEO of Audax Strategic Advisors. (kthoren@kth.se)

Kiitokset: CKIR, ETLA ja raportin kirjoittajat kiittävät Business Finlandia *Mobile is Global* -projektin tukemisesta (Diaari Nro 3265/31/2024).

Acknowledgements: CKIR, ETLA, and the authors wish to thank Business Finland for its kind support of the *Mobile is Global* project (Diary Number 3265/31/2024).

Avainsanat: Mobiili televiestintä, Teknologian käyttöönotto, Geopolitiikka, Geotalous, Teknologinen suvereniteetti

Keywords: Mobile telecommunications, Technology adoption, Geopolitics, Geoeconomics, Technological sovereignty

JEL: O33, L52, L96

Contents

1 Setting the scene 4
2 Introduction 8
3 Context 9
4 Nordics 9
5 Ecosystem 10
6 Use cases 11
7 Technology 12
8 Regulation in the EU 19
9 Regulation in Finland 21
10 Conclusions 23
Endnotes 24
Literature 27

1 Setting the scene

On the project

This is the opening report of the *Mobile is Global – How the new geopolitics influence the 5G and 6G industry and the Finnish innovation ecosystem* project, which is a collaborative research effort of *Aalto University*'s *Center for Knowledge and Innovation Research* (CKIR) and *ETLA Economic Research*. The project is kindly supported by *Business Finland* (Diary Number 3265/31/2024).

The *Mobile is Global* (MiG) project
- assesses geoeconomic realities influencing developments in mobile communications,
- offers a roadmap to reduce future uncertainties, and
- provides recommendations for paths forward for Finnish and European policymakers and industry.

MiG consists of five work packages, of which this report mostly relates to the first.

The purpose of this report is
- to establish the context for the project,
- to highlight key issues, and
- to serve as a starting point for the other four work packages.

On the title

Our title *5G in the Era of Geoeconomics: Playbook for Finland?* calls for an explanation.

Even though we are thinking of the future of mobile communications, we label the discussion by its fifth generation (5G) – just to be concrete in our thinking.

We are thinking of mobile communications via successive, overlapping generations defined by applicable national and international technical standards that – after establishment and roll-out – span a diverse and large system of private and public actors.

While the evolution of mobile communications has been greatly molded by nation-states as well as government and international agencies, in the past its most successful aspects have been driven by private businesses that both collaborate and compete internationally.

This competition has been mostly fair in the sense that technical merits in standardization and in provision of gear have carried weight and that providing superior customer value has tended to translate into respective providers' growing market shares. The consequences have been fast technical evolution and rapid adoption, which in turn has provided large societal benefits.

Geoeconomics, which we define as international power politics by economic means, has been reasonably remote from 1G to 4G but is quite prominent in 5G – and most likely in future generations of mobile communications.

As for the *Playbook for Finland?* subtitle, we indeed focus on Finland but consciously thinking of any similar small, open economy – most notably also Sweden. Despite the subtitle, we address mobile communications as a global phenomenon – with a distinct European focus.

The subtitle is posed as a question: Does Finland need a (new) playbook in this context? If so, what should it look like?

Since this is the opening report of our project, the purpose here is rather to set the stage for our subsequent efforts than to provide definite answers.

Geoeconomics

Amano Tatsushi of JBIC[1] defines **geopolitics** as "realism" and **geoeconomics** as its "economic means".[2] Realism refers to his grim view that nation-states use any means necessary to pursue their interests and that cross-border dependencies are increasingly interpreted as national vulnerabilities.

Wigell et al. (2022, p. 12) suggest that in "... the broadest sense, geoeconomics is the pursuit of power politics using economic means. This includes measures such as embargoes, sanctions, export controls, anti-competitive subsidies, investment screening mechanisms and data localization measures." The word power here suggests that Finland rather adapts to than influences how geoeconomics plays out, although the EU at large is of course a sizable player.

Wigell et al. (2022) note that geoeconomics affects business enterprises at three levels:

1. market segments and even entire countries may become no-go business areas;
2. competitive dynamics change, as political preferences shift towards national champions; and
3. geoeconomics needs to be embedded into business strategies, when governments increasingly intervene in cross-border flows of goods, services, capital, people, and information.

The Wigell et al. (2022, p. 35)[3] definition of geoeconomics borders on conducting "war by other means", which the authors (p. 21) indeed make explicit: "The weaponization of economic relations refers to the increasing trend of harnessing and disrupting economic relations to gain strategic and national security advantages."

The above sounds as the **opposite** of the three-decade *great moderation* era of globalization that prevailed until the eve of the 2008–2009 great financial crisis. In this era, deepening cross-border ties were seen not only as a source of economic prosperity but also as a way to alleviate tensions among nation-states, i.e., as a means to achieve better national security.

If economic weaponization is taken to its logical conclusion, it implies that nation-states would have no cross-border interaction at all.[4] This impossibility brings us to consider a meaningful interpretation of national security and other interests in the context of 5G.

National interest

To discuss analytically how geoeconomics and 5G mix, we need to define explicitly what Finland seeks as a nation-state.

Geopolitics is closely aligned with national security. Geoeconomics certainly relates to national security but, in our thinking, it also aligns with other interests, such as national prosperity.

While we find it difficult to define Finnish geoeconomic interests in general, doing it in the context of 5G appears straightforward – via a simple split in Exhibit 1:

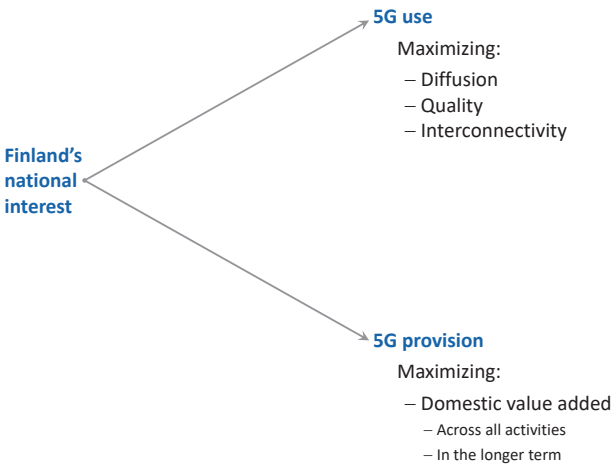
- **5G use**: To maximize the positive societal impact on the side of 5G use, we want the most widely available and the highest quality infrastructure with the lowest possible costs of build-up and operation.

- **5G provision**: Building up, operating, and providing services over 5G offers a wide range of domestic and international business opportunities. The interest in 5G provision is to maximize generation and capture of Finnish national value added. Even though here we are in the context of 5G, this maximization should take place across **all** economic activities – in other words, if resources are best employed in other lines of business, the implication could well be that Finland has less interest in 5G provision.

In both 5G use and provision, national interests should be understood in terms of net present value – evaluating not only immediate costs/harms and returns/benefits but also how they evolve over time.

Trade-offs need to be considered in addressing national interests. A nation-state has every right to pursue sovereignty in technology and in the provision of goods and services but, in a world utterly dependent on geographically dispersed production, sovereignty comes at a cost: on the positive side, interconnectedness via global supply chains (and specialization it implies) makes us more prosperous as long as cross-border links are intact – on the negative side, interconnectedness makes us vulnerable in less fortunate times.

Exhibit 1 Finland's national interest



Source: The authors' illustration.

Because interest in 5G provision spans across all economic activities, Finnish interest here is somewhat muted and may primarily focus on business activities directly related to 5G use.[5]

Four implications

The previous section implies four core domains of Finnish interest in 5G:

- **Speedy and widespread diffusion**. Having predictable and supportive investment and business environment.
- **Low build-up and operating costs**. Promoting private competition while also avoiding wasteful replication.
- **Robustness against internal and external threats**. Addressing attack vectors that could reasonably compromise availability of service.
- **Keeping data secure**. Understanding what data and security in 5G mean. Considering legislative and technical means to address cybersecurity.

Attack vectors

Internal and external threats could be mediated via myriad of attack vectors over the life cycle of mobile communications from establishing governing legislation, spectrum allocation, and standard setting all the way to the stage when infrastructure and devices are retired from service.

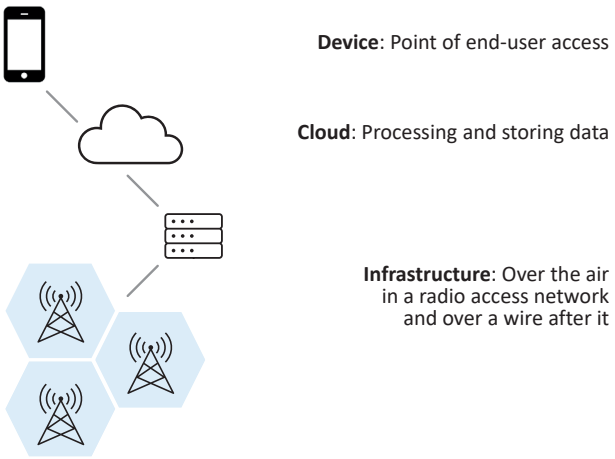
In real time, threats and attack vectors relate to the current operational infrastructure as illustrated in Exhibit 2. An attack could be aimed at compromising the whole infrastructure or some of its users.

The chain in Exhibit 2 is truly as strong as its weakest link. Most known attacks have happened at a device or via direct (cloud) service provision to it. Thus, strictly speaking, they fall outside 5G.

At the level of the infrastructure, provider diversity, certification and testing, end-to-end encryption, and verification of content and data are among deployable security features.

The infrastructure itself faces risks – e.g., the possibility of physical sabotage and natural phenomena such as solar storms – beyond what is implied above. With increasing dependence on mobile connectivity, this risks extend to other areas such as health care and smart grids.

Exhibit 2 Attack vectors



Source: The authors' illustration.

Data onion

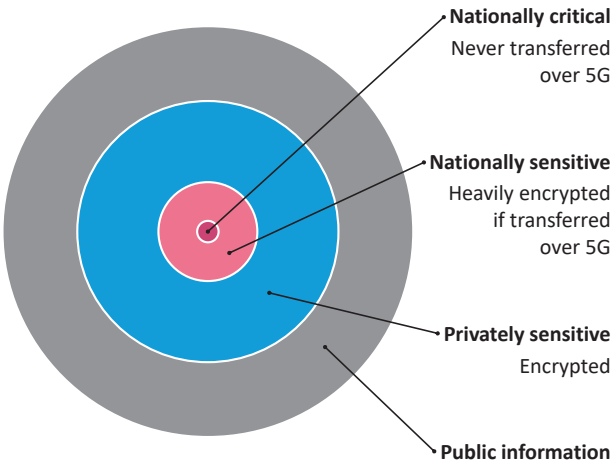
Essentially all information and communication technology (ICT) is dual use, i.e., it has both civilian and military applications – no wonder that, e.g., NATO has keen interest in 5G.[6]

Applying military logic to the fullest implies that one should not rely on foreign entities at all. If such logic is applied to 5G, a small open economy could not have mobile communications at all, since complete domestic provision is not feasible (at an acceptable cost).

Dual use also applies to data. For example, social media posts and geolocations from heart rate monitors can be used in espionage. In times of war, a soldier's careless opening of a mobile phone is an invitation for enemy fire. Also in the case of data, applying military logic to the fullest leads to an impossible conclusion that no data should be publicly available.

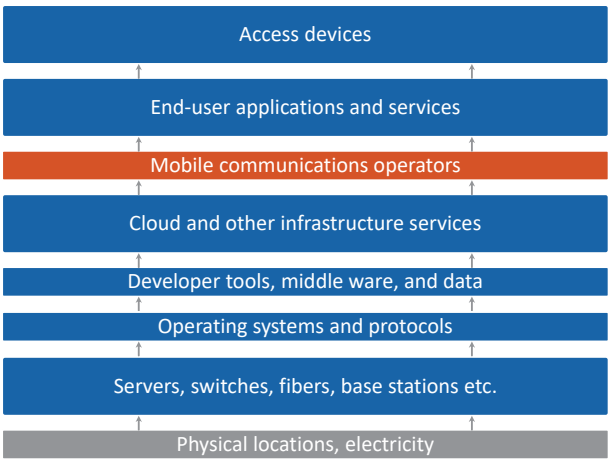
In Exhibit 3, we suggest thinking of national data security interests as layers of an onion. The most nationally

Exhibit 3 Data onion



Source: The authors' illustration.

Exhibit 4 5G infrastructure stack



Source: The authors' illustration.

critical information never rides on public infrastructure, so it falls out of consideration in the context of 5G. The second tier, nationally highly sensitive information, does ride over public infrastructure, but in a heavily encrypted form and between dedicated terminals.

The outermost layer in Exhibit 3 concerns information that is, from the outset, publicly available.

With the above logic, the primary 5G data security concern is in fact in the layer that we label privately sensitive in Exhibit 3; its security is still imperative but addressing it is less of a hurdle than in the inner layers.

Stack

A stack is a standard way of thinking about interrelated aspects of an ICT infrastructure. At the bottom of a stack, one typically finds physical underpinnings such as fiber-optic cables; final uses are found on top.

In Exhibit 4, we have drawn one version of the 5G stack. Even at this broad level of aggregation, 5G is quite complex. Each level has somewhat different geoeconomic and security concerns and spans its own set of attack vectors.

In our view, the four implications above suggest that mobile communications operators – towards the middle of the stack in Exhibit 4 – are crucial in fulfilling national interests when it comes to 5G.

Dynamic view

The stack provides a valuable framework for considering ICT infrastructures; however, it is limited by its inherently static nature. National interests in 5G need to be thought about in terms of net present value and over the long term, i.e., dynamically.

A new generation of mobile communications starts with setting at least some design principles and allocating spectrum for future purposes. This planning is initiated decades before a commercial roll-out of infrastructure and devices. Thus, assuming a dynamic view means that a nation-state (and a regional body, e.g., the EU) must plan ahead and anticipate consequences of its actions decades ahead.

Policy

In the context of 5G, societal policy operates via four levers:

- Who has access to resources such as spectrum, geographical locations, finance, and human resources?
- What are the fields of (private) competition and on what terms competition takes place?
- What are the possibilities for interoperability and for offering services and solutions riding on the infrastructure?
- What choices, rights, responsibilities, and degrees of freedom do end-users – both businesses and individuals – have?

National policy making, addressing the above questions, takes place in an international context illustrated in Exhibit 5. International law and the established international mobile communications standardization apparatus is found on top and, with our perspective emphasizing 5G use, the most important part – mobile communications operators – are found at the bottom. Lobbyists also play a key role in shaping 5G policy at both national and international levels, influencing everything from global standards to national implementation and pushing the interests of telecom operators, tech firms, and other stakeholders into policy decisions.

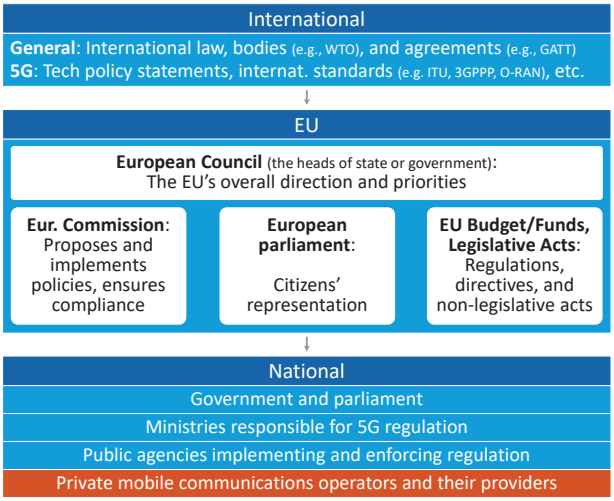
Value creation

Both in the regulatory and business side, ultimately the fundamental driver of developments in mobile communications is, in our view, economic value creation.

As is typical in earlier stages of technological development, value creation is more intense towards the bottom of the stack and then moves upwards over time.

In the earlier generations, much of the value creation was in handsets and in applications and services that directly ran on them. Currently, much of the value in the stack is in the utilization of data. Communications networks are the fundamental enabler in making the data available as well as in enabling data-based value creation.

Exhibit 5 Regulatory structure



Source: The authors' illustration.

Tools for thought

The purpose of this section has been to provide some tools-for-thought and a frame of reference for reading the remainder of this report.

In this section we have:
- Given a specific interpretation of Finnish national interests in the context of 5G.
- Shared some thoughts on attack vectors of internal and external threats.
- Introduced a data onion for thinking of data security.
- Used the 5G stack to suggest that core Finnish interest might be in a specific layer of it – mobile communications operators.
- Framed out dynamic view on societal 5G policy and given a flavor of the international context in which it takes place.

2 Introduction

In the late 1990s and early 2000s, mobile telephony was a domain in which international coordination and collaboration was exceptionally intense and successful. By the advent of 4G, the world managed to nurture a single and nearly perfectly interoperable mobile communications standard/infrastructure that became to blanket the earth.

Today, with an estimated 7.41 billion global users,[7] mobile telephony is arguably the most foundational technology for all societies. With this, future evolution of mobile communications is fundamental to all countries – particularly for the ones that play a role in providing these technologies.

Late in the Obama administration (lasting until 20 Jan. 2017), technology became the focal point of geopolitical tensions between China and the United States. Early in Trump's first presidency, the emphasis was on big data and platforms but then 5G became the primary flashpoint. Even though the flashpoint upon writing this in late 2024 is artificial intelligence, the US trade restrictions against China remain the most intense in the context of 5G, as manifested by a broad and long-lasting blockade of Huawei – previously a leading global 5G provider.

The EU's and its Member States' roles in the US' and China's ongoing geopolitical struggle is ambiguous. It has traditionally aligned with, and depended on, the US on matters of defense and security. However, both the EU and its Members do have distinct national interests.

In the current era of increasing lawlessness and mudslinging in international relations, especially small, open, and tech-driven economies – such as Finland – must carefully consider, what national strategies and policies best support citizens' future prosperity (For discussion, see Ali-Yrkkö et al., 2024).

3 Context

Up until the late 1990s, digitalization largely fell under three categories,

- telecommunications,
- computers/electronics, and
- media/content,

all with their own providers and operators. In public policy, the three were considered separately – and largely nationally.

In the postwar era, telecommunications have gone from a public utility, often run by a state monopoly, to relatively open competition among numerous private companies. Within telecommunications, mobile telephony formed its own vertical up until the early 2000s. Since then, however, we have experienced rapid technology convergence.

With 5G, mobile communications is increasingly a general-purpose technology – like steam over 200 and electricity over 100 years ago – forming the backbone of the all-IP (Internet Protocol) world.

Perhaps the most important use case for 5G is *Internet of Things* (IoT) and *machine-to-machine* (M2M) communications, which are both crucial to, e.g., autonomous logistics and virtualized health care.

While widespread global deployment of IoT/M2M is still ahead of us, it is seen as a pivotal step towards a truly connected society. This would create a digital version, or a digital twin, of our physical world, mirroring it in real time (for discussion, see NTT DOCOMO 2023).

Already, more than half of Internet traffic originates from mobile devices; most bits/data touch upon mobile communications infrastructures at some point of their existence. The widespread use of mobile technology has enabled online services and apps to reach massive user bases at unprecedented speeds, accelerating product life cycles and adoption rates. For example, while Netflix took 3.5 years to reach a million users, ChatGPT achieved it in five days, and Threads in just one hour.

Over the last twenty years, mobile-driven connectivity has fueled the raise of gigantic American (e.g., Apple, Google, and Facebook) and Chinese (e.g., Alibaba, Baidu, and Tencent) platform companies.

Digital platforms are central to the 5G story, since they are the primary means of collecting vast amounts of data on essentially all individuals and organizations. And, to make use of the data, platform companies are among the leading developers of artificial intelligence, which in its own right constitutes a transformational general-purpose technology.

The complicated interaction of 5G, platforms, data, and artificial intelligence has brought privacy and security issues to political agendas in virtually all countries and regions. The major players – the US, China, and the EU – have chosen quite different political and regulatory paths into an information-driven economy (for discussion, see Harakka, 2023).

4 Nordics

The evolution of the mobile communications industry is an interesting, and quite Nordic, saga.

In year 2000, Nokia's direct share of Finnish GDP peaked at 4%, which the respected British business periodical The Economist called the world record for a single company (outside oil- and other resource-dependent countries).[8] At the same time, Ericsson's share of Swedish GDP was 2%. Since Sweden is twice the size of Finland as an economy, moneywise Ericsson's and Nokia's

roles were about the same. Even today, the two companies are nationally important.[9]

Ericsson and Nokia loomed large thanks to intense public-private collaboration in nurturing the *Nordisk Mobil Telefon* (NMT, a first-generation mobile standard, 1G) standard since the late 1970s and in particular thanks to the first European, and ultimately global, *Groupe Spécial Mobile* (GSM, a second-generation mobile standard, 2G) standard developed since the late 1980s.[10] With over 50% of all standard-essential GSM patents, Nokia and Ericsson cemented their influence in the mobile infrastructure market and solidified their industry leadership.

In the subsequent 3G and 4G standardization rounds things got messier and more politicized, even though the same basic setup was still applied; in standardization and essential patents, the US and Qualcomm became to the forefront at the expense of Ericsson and Nokia.

A standard is a bundle of agreed technical solutions and interfaces, which need to be embodied in compatible goods and services to generate business and economic value added. Countries that plan to be just users of technology are not in a rush to implement it; the ones that want to be providers of technology want to be among the first implementors in order to lock in precious fast-mover and early-adopter advantages – this is exactly what Sweden and Finland did with 1G and 2G.

In 5G, China, and particularly Huawei, followed the GSM-era examples of Ericsson and Nokia. Huawei invested heavily in R&D and standardization processes. It worked closely with academic institutions worldwide (Yan & Huang, 2022), also something that its Nordic peers cherished early on.

5 Ecosystem

Suraci et al. (2021) comb scholarly literature to identify 5G stakeholder groups. Exhibit 6 features their classification. The authors note that a (licensed) mobile network operator's role is quite complex in the literature – and arguably even more so in real life –, although a useful and often sufficient simplification is to consider separately the ownership of infrastructure and the operation of its service provision.

Fransman (2010) offers another way to categorize 5G ecosystem actors. In his view (Exhibit 7), there are four groups of entities: Since 1G, features of the air interface have not only defined the generation but also spanned a distinct group of stakeholders. Applicable regulations (e.g., net neutrality) induce separations of networks/infrastructure and services/devices. What rides on a net-

Exhibit 6 5G stakeholder groups as recognized in scholarly literature

Stakeholder	Description
Hardware and software providers, equipment manufacturers	Provision of network infrastructure components
Infrastructure providers (and other suppliers) of mobile network operators	Ownership and lease of assets "as a service" (without operating)
Mobile service providers	Operation of infrastructure (without owning)
Mobile network operators	Ownership and operation of mobile communications infrastructure (a combo of above two)
Tenant	Reseller of virtual network resources
Service provider	Offering services to consumers (this role can be played by several entities)
Developers	Creation of applications for various stakeholders
Over-the-top services	Service providers on top of the network (e.g., Facebook, Netflix, and YouTube)
Brokers	Mediation between stakeholders (e.g., in negotiating service level agreements)
Subscribers and end-users	Final consumption of infrastructure-supported services
Others: verticals (e.g., health care and transportation), SMEs, startups, public bodies, standardization bodies, end-user equipment manufacturers	Either benefitting from infrastructure services or participating in infrastructure development

Source: Chiara Suraci et al. (2021, Table 1 – with modifications).

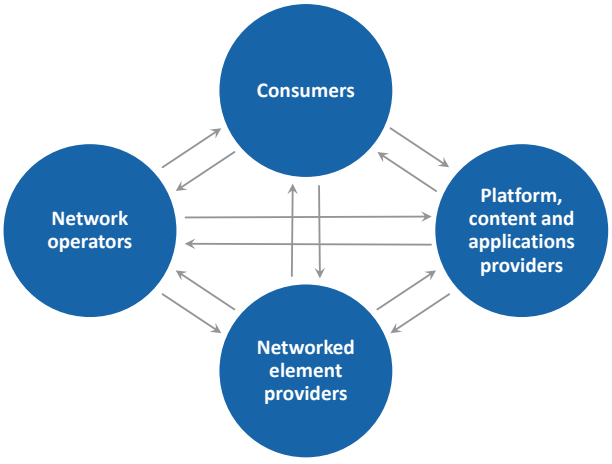
work and devices used to access it – content of all types and (meta)data –, further spans other groups of stakeholders.

The 5G ecosystem's complexity is somewhat reduced when looking at it at two levels of abstraction. At the higher level, vendors, manufacturers, operators, and other complementary actors together ensure the existence of communication functionality by providing an accessible and reliable infrastructure. Their main collective function is, to play on Nokia's old slogan, to connect people (and organizations). Security, maintenance, and other functions are, at this level, support functions necessary for the main function to work as intended, but not the reason an infrastructure is built. Connective functionality then becomes a contextual asset in the overall innovation ecosystem in which a multitude of other actors exist (Exhibit 6), including developers, service providers, OTT companies, and all other actors that have business models that rely on connectivity for their value propositions (i.e., beyond their normal daily communication needs).

Many of these are, in turn, connected with each other and external actors in the production and delivery of a value proposition that none of them could effectively achieve alone. In other words, the innovation ecosystem supports a number of business ecosystems which are clusters of actors that generate customer value together (Hannah & Eisenhardt, 2018; Valkokari, 2015). Each of these actors has a business model that (leverages assets to) contribute with some function to the others in the network or to the end customer.

Innovation ecosystems are wider, and their output is innovations, i.e., new value propositions. Business ecosystems, on the other hand, are set up to realize the value of earlier innovations. However, when a new technology, such as 5G, becomes available in an innovation ecosystem it allows value creation to reach higher levels. Primarily, new technology has this effect by removing existing constraints, thus making new innovations possible (Normann, 2001). These innovations, when manifesting as new value propositions, can make previous business ecosystem functions redundant and require new ones to be added, often resulting in structural changes in ecosystem role dependencies (Thorén, 2021).

Exhibit 7 5G stakeholders and their symbiotic relationships



Source: A slightly modified version of Exhibit 3 in Fransman (2010, p. 37).

6 Use cases

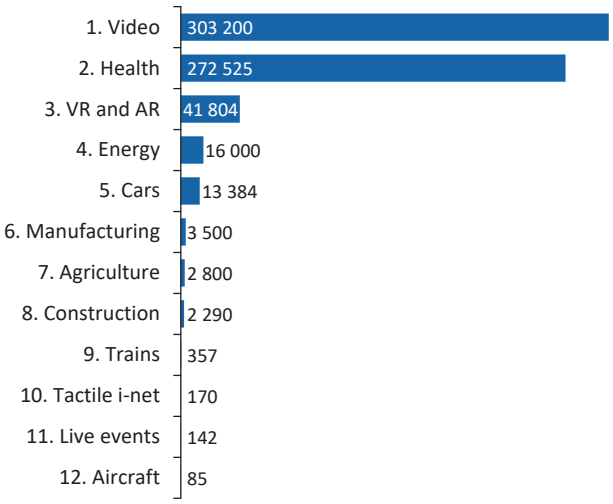
In thinking of 5G use cases, the emphasis should be on examples were having an over-the-air link is crucial, as otherwise the topic converges to a general discussion on digitalization.

While a human on the move, e.g., in a car, is a typical example, a use case may well happen in a narrowly defined geographical environment. For example, an automated underground drilling rig needs wireless connectivity, albeit only in a well-defined 3D space spanned by mineshafts.

While pilots, demonstrations, and even day-to-day applications are certainly among us, the analysis of 5G use cases and "killer applications" still involves educated guesswork, as they are mostly in the future.

Hoeschele et al. (2021) provide an interesting holistic model deriving the overall importance of various 5G use cases. Based on their systematic approach, they derive a per-application overall impact rating (with Rating ρ measuring how a particular 5G application affects the traffic levels at the core Internet). Based on this rating, video, health, and virtual and augmented reality are the most important use cases for 5G (Exhibit 8).

Exhibit 8 Relative inter-domain traffic impact of 5G use cases, Rating ρ value



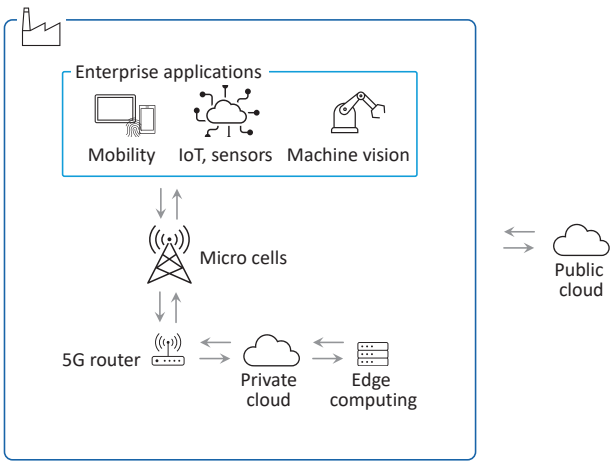
Source: A modified version of Hoeschele et al. (2021, Table 5).

One of the main ways of distinguishing 5G from the earlier generations is its support for private networks that seamlessly interact with the publicly accessible infrastructure.[11]

Exhibit 9 is a semantic illustration of what an implementation of a 5G private network might look like in the case of an industrial site.

Eckard Eberle,[12] CEO of Global Business Services at Siemens, has noted that "Industrial 5G is the gateway to an all-encompassing, wireless network for production, maintenance, and logistics. High data rates, ultra-reliable transmission, and extremely low latencies will allow significant increases in efficiency and flexibility in industrial added value."

Exhibit 9 An illustration of a private 5G network implementation of a factory



Source: A slightly modified version of Accenture's illustration.[13]

7 Technology

5G is a set of technologies embedded into internationally agreed technology standards that – with the necessary further steps of allocating radio spectrum and building infrastructure – provides functionalities for compatible devices' over-the-air communications.

5G may be characterized by a few key dimensions:

- **Enhanced mobile broadband**. Ultra-high bandwidth and speed enabling, e.g., bi-directional communication required in high-definition video calls and in augmented reality applications involving real-time exchange of information on a user's surroundings.

- **Massive Internet of Things**. Potentially millions of over-the-air connections in a small geographical area, e.g., on a process industry site with sensors for each valve and pipe segment.

- **Mission-critical services**. For example, in the future, autonomous vehicles might drive within a few centimeters of each other to save energy – a signal for breaking must be deliverable instantly 100% of the time; intense health care units may have wearable sensors on patients; a warning of a stroke must be extremely rapid, as fractions of a second matter for longer-term health outcomes. Especially the former example combines the need for ultra-low latency (a minimal delay in transmitting a backet of data) with ultra-high reliability (i.e., no losses of or variations in connectivity).

- **Integration into all other forms of digital communications** from fixed broadband to satellite.

Architecturally, the above implies that the network must be software-based and that the managements of both demand (user needs) and supply (resource allocations in

terms of spectrum etc.) must be very nuanced and timely, which is impossible with either a priori set rules or human effort – implying that artificial intelligence is needed for 5G to fulfill its promises.

With a software-based implementation, operators can "slice" the network for different types of uses as well as lease out "virtualized" resources, say, something that looks like a private wireless intranet with a company's own server.

More broadly, the operation of the network is largely disentangled from the physical infrastructure – while 5G is not a pure cloud computing infrastructure,[14] it largely applies the same underlying principles.

If the need-for-speed in delivering data packets is paramount, pursuing central processing might become physically impossible. The need for an ultra-quick response – implying ultra-low latency – gives rise to edge computing, where processing happens closer to the point, where data is collected and where the outcomes of processing are needed.[15]

In some ways, 5G is just bigger and better.[16] As compared to 4G,

- It can handle large volumes of over-the-air (data) traffic at fast speeds.
- It has low latency (delays in transferring packets of data).
- It has (nearly) complete geographical coverage.
- It has a constant quality of service (the guaranteed level of which may vary from use to use).

However, 5G also has features beyond 4G:

- 5G is the first mobile generation to fully embrace cloud computing principles and to be comprehensively software-defined.
- 5G can deliver a massive number of simultaneous connections (IoT and M2M communication are 5G's founding principles).
- 5G is more open (e.g., enhanced support for private sub-networks) and it has more distributed networking capabilities (e.g., edge computing).
- 5G can define and service industry (e.g., health care) and other "verticals" (with specific features and different value propositions for, e.g., autonomous vehicles and tracking devices).

4G is a "one size fits all" solution. 5G differentiates across various uses and across resources deployed in serving them and is – from the outset – designed to serve both humans and machines, arguably with emphasis on the latter.[17]

Even though 5G provides jump in energy efficiency (relative to data volume), with increasing numbers of devices and data volumes, environmental friendliness becomes a concern.

5G enables environmental actions in other domains. For instance, better management of transport and traffic lowers capacity needs and energy waste; the circular economy exploits IoT to enable Product-as-a-Service business models and reuse.

History

The evolution of mobile "cellular" telephony started (the 1st generation, 1G) in the late 1970s and the early 1980s with analog standards, such as the afore-mentioned NMT, that were almost exclusively designed for human voice communications (largely in situations where wireline connectivity was not available).

In the early 1990s, the fundamental shift from 1G to 2G – globally mostly based on the afore-mentioned European GSM standard – was a move from analog to digital technology. During 2G, mobile telephony moved from corporate and wealthy private customers to almost universal use in the developed countries and to the upper- and middle-classes of the developing ones. 2G remained voice-centric with some support for data communication – arguably SMS messaging was 2G's "killer application".

With 3G in the late 1990s, revenue-wise voice was still in the lead, even though 3G's signature feature was (limited) mobile broadband and thus support for mobile multi-media use. Only with 4G – on the eve of the 2008/9 financial crisis – did mobile broadband become truly ubiquitous and usable; with this, data became the primary source of operators' revenues. As far as data volumes go, streaming video is 4G's killer application.

The 4G to 5G extensions are discussed above. To summarize, 5G is an integrated approach to digital connectivi-

ty; 5G serves as a hub or a "network of networks" covering not only cellular but also other mobile connections (e.g., satellite) and wireline.

Throughout the technology generations, the basic division of labor among actors has been intact: regulators set the "rules of the game"; cooperative bodies set standards; equipment manufacturers provide technical solutions and gear embodying them; and, broadly speaking, operators purchase, own, operate, and secure networks.

Infrastructure

A country's communications infrastructure may be split into fixed-line Internet and mobile communications. Historically, the former emerged around computers and the latter around telephony, although during the 2000s the distinction between fixed and mobile is increasingly a line drawn in water.

A fixed communications network may be thought of as a branching tree (Exhibit 10), although in practice a network is less hierarchical. From a network operator's point of view, its highest level and the starting point is the core, which may be understood as a central switchboard (akin to the trunk of a tree). The main branches forking out of the core are the next level; these branches and their sub-branches are what is collectively called the metro (as the name referring to a city suggests, these are relatively large segments of the network). The final nodes in the network, i.e., what is inside a building of final use as well as cables and equipment directly leading to a building, are collectively called the access.

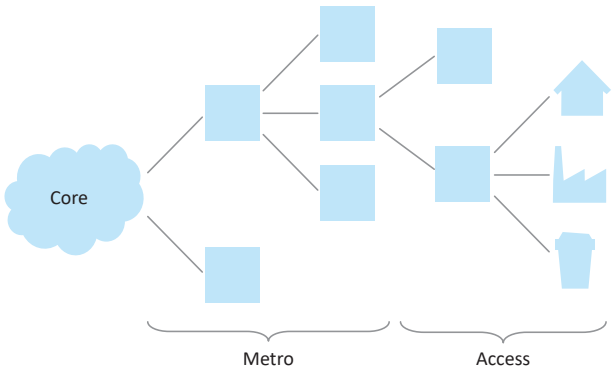
A mobile communications network is characterized by the use of radio spectrum in transmitting bits – both voice and data. Due to the iron laws of physics, radio spectrum is a scarce resource. Thus, to transfer large volumes of bits, a mobile network is based on geographically bound cells, which enable the use of the same spectrum in other geographies. To provide uninterrupted service to a user on the move, adjacent cells need to be able to hand over data traffic on the fly.

The radio access network (RAN) is the only over-the-air part in a mobile communications network (Exhibit 11); the rest is based on landlines in a similar manner – and partly exploiting the same infrastructure –, as in the case of a fixed network.

As its name aptly suggests, the core is the most important part of the infrastructure, as it ensures that end nodes in the network (humans or machines) can connect and exchange information. Key aspects of access management and traffic allocation happen at the core and data is mostly stored and processed there.

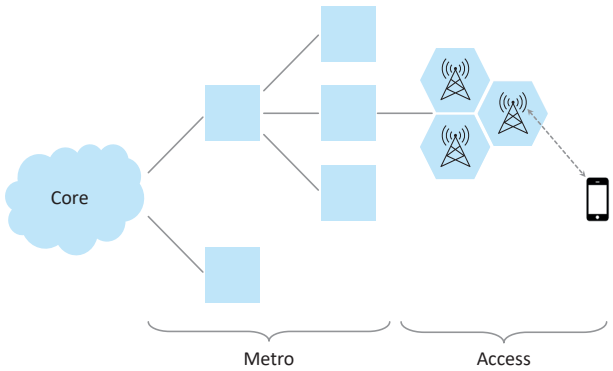
Fixed and mobile communications operators control their infrastructure and traffic within them; equipment vendors sell hardware and software to operators but are not in charge of running the networks (save it for tasks operators' choose to outsource).

Exhibit 10 A stylized view of a fixed communications network



Source: The authors' illustration.

Exhibit 11 A stylized view of a mobile communications network



Source: The authors' illustration.

A real-world 5G infrastructure is more like a spider web than a branching tree illustrated in Exhibit 11. However, it does retain the elements of the core, metro, and access, even though, e.g., the introduction of edge computing (not to mention other complications such as network slicing) makes the definitions of these hierarchical elements cumbersome.

With the above, it should be clear that digitalization relies on a vast network of physical infrastructures ranging from satellites and submarine cables to a diverse set of access points from phones to refrigerators. The control of, and software-mediated access to, these infrastructures convey a form of (mostly dormant) power that has implications on national interests.

A further complexity in a mobile communications infrastructure is that various generations of mobile technologies are simultaneously in use and that they employ multiple spectrum bands. Thus, operators need to optimize over multiple standards and bands. Since interfaces needed for this optimization do not function smoothly across network gear vendors, operators are torn between resorting to just one vendor and incurring extra cost due to multiple ones.

Spectrum

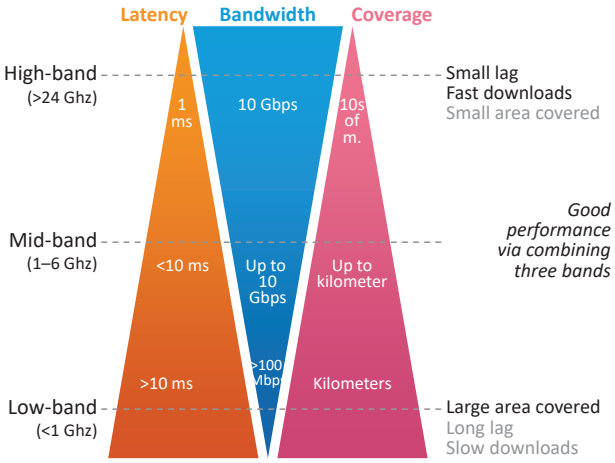
Only a small, albeit foundational, leg of 5G happens "in the air" over multiple radio frequencies, the continuum of which is collectively called the spectrum.

Spectrum is best thought of as a fixed series of local frequency pipes; techniques can be used to pump more stuff into them, but eventually there is an inescapable physical limit.

5G depends on governments and regulators granting timely access to the right amounts and types of affordable spectrum.

As data volumes grow, 5G will also depend on the real-time optimization in the use of spectrum – the new and difficult aspect in this is that this optimization ought to happen across spectrum licensees, which are independent private enterprises.

Exhibit 12 5G operates across three bands of spectrum



Source: A modified version of Boston Consulting Group's illustration with Forbes, IC5G, IMT-2020, OpenSignal, and Verizon mentioned as BCG's original sources.[18]

The properties of a radio frequency are determined by its wavelength. 5G uses three archetypes of spectrum: the low-, middle-, and high-band (Exhibit 12). Frequencies in the high-band travel short distances and are easily absorbed by physical obstacles or rain; on the positive side, they can support large volumes of fast-moving data with miniscule delays in transmission. Low-bands are the opposite of high-bands in all these respects. The characteristics of the bands are mirrored in infrastructure and in use cases.

Standards

To work from end-to-end globally, 5G needs to be supported by hundreds of internationally agreed-on technology standards, which are in essence blueprints on how disjoint and modular elements interconnect to enable bi-directional communication and service provision among humans and machines.

In 5G, standards are mostly about interconnection protocols and interfaces; what happens "with-in a module" is typically left to a provider and might thus be proprietary.

3GPP, the 3rd Generation Partnership Project, was established in 1998 as an umbrella body of several telecom-

munications' standardization bodies (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, and TTC) for the process of nurturing 3G. With later generations, the 3GPP has continued to serve in the same role.

Requirements

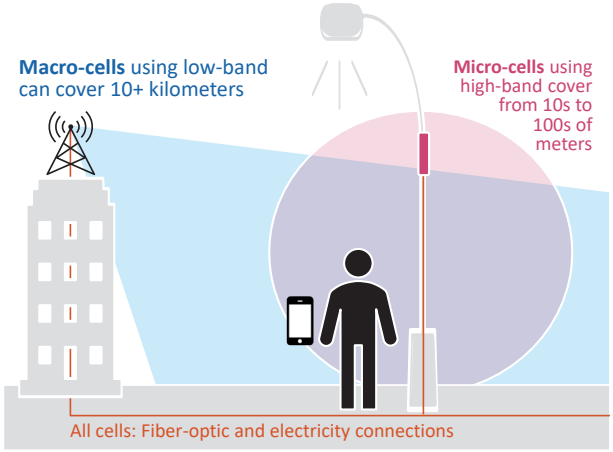
5G uses multiple radio frequencies that have different abilities to move over-the-air and to penetrate physical obstacles.

A mobile network consists of geographically bound cells that need to combine/overlap for seamless connectivity on the move.

The low-band can serve "macro-cells" from base stations several kilometers away; the high-band needs "micro-cells" and base stations that are within a few hundred meters from the point of use. With multiple deployed frequencies and varying needs of application verticals, the physics of a 5G network are best thought of as a multi-layered mesh (Exhibit 13).

As Exhibit 13 illustrates, every base station needs a fiber optic connection. Current fiber-optic cables, called the backhaul in the context of 5G, are insufficient for mobile communications' future needs.

Exhibit 13 Macro-cells using low-band and micro-cells using high-band complement each other



Source: A modified version of an illustration in Smart Docklands report.[19]

In the context of 4G, operators mostly have (or lease) their own (macro-cell) towers, base stations, fibers etc. Furthermore, these are only in part shared with fixed network infrastructures. With 5G, it is increasingly in question whether separate infrastructures are sensible or even feasible, which is an issue that regulators must also consider.

A further complication is that 5G is indeed to serve as a "network of networks" beyond its considerable own capabilities; the joint initiative of the European Commission and the continent's ICT industry notes that "The 5G concept combines various access technologies, such as cellular, wireless, satellite and wireline, for delivering reliable performance for critical communications and improve area coverage".[20] Circa 2030, we might no longer talk about 5G and the internet independently, as the two have merged into each other. Thus, all digitalization-related regulatory issues will also be 5G issues.

The realization of 5G will be quite different from all the earlier generations of mobile communications. This also disrupts earlier regulatory frameworks. On one hand, 5G needs to be much more collaborative and it needs to embed fluid sharing and shifting of resources. On the other hand, it needs to be conducive to innovation and competition – in a context where some future trajectories are simply unknown. It is even hard to grasp what and who to regulate: as far as 5G infrastructure is concerned, there are no clear lines of command and control but rather multi-party contractual arrangements involving dispersed and overlapping ownership structures and service obligations.

Regulation

5G's performance requirements and technical aspects have direct implications on regulation.

The bottleneck of spectrum will ultimately be severely binding. In the context of spectrum, national and international regulatory questions are:

- How to make the maximum amounts of different frequencies available?
- How to ensure optimization and sharing in use, while supporting innovation, competition, and private incentives to invest?

- How to maximize societal netgains – perhaps, e.g., including balancing between immediate public revenue from spectrum auctions and consequences that it might have on network roll-out and use?

5G's infrastructural needs are large in terms of:
- physical access points (base station locations),
- hardware and software gear, and
- monetary investment.

In a world increasingly influenced by geoeconomics, these needs are addressed in a much more uncertain, unpredictable, and unforeseeable world.

With 4G, operators would negotiate and contract with land and property owners separately for each (macro-cell) location. This will not be feasible in 5G. Regulatory measures are needed for ensuring, from the operators' point of view preferably automatic, "rights of way" in deploying base stations, backhaul fiber-optics, and electricity connections. Most locations will be on public land and infrastructure.

As for provision of gear, generally society is best off by having open, competitive, and – outside commonly set standards – technology-neutral markets at each level of the technology stack.

As far as private investment is concerned, previously the approach has been to introduce a new generation in the marketplace and to "see what happens". With future generations, investment needs are larger and return more uncertain. Consequently, 6G (and beyond) might have a chicken-and-egg problem: a "push" strategy, building a full infrastructure and waiting for (sufficiently profitable) use cases, has a long and uncertain payback; whereas a "pull", i.e., customers' demand (in large volumes and with a high willingness to pay), might not emerge before a technology is fully deployed. In such a context, enabling and motivating private investment is also a public concern.

In 1G to 4G, the network coverage and speed provided at each location has been determined by operators' business logic; with 5G, this is not necessary socially (or politically) desirable. The argument is similar to "fiber socialism" that – mostly at the municipal level – has been applied in many European countries: if and when (mobile) digital connectivity serves as a gateway to many public services and supports democracy and other socially desirable objectives, certain quality of (mobile) connectivity is a "fundamental human right". Just applying business logic will leave some areas out-of-luck, which might be unacceptable from a social viewpoint.

Competition in the context of 5G is a tricky regulatory issue. With 5G, there are several economic forces promoting market concentration. Both economic (scale and scope economies) and technical issues (spectrum optimization and physical infeasibility of multiple infrastructures) point towards cooperative build-up of infrastructure and sharing of resources upon operating networks, which in turn change the locus of competition as compared to 1G to 4G.

In 1G to 4G, regulation has often been based on the idea that there is one type of intermediary to regulate. In 5G, the policy challenge is that (a) the earlier "silos" now converge into the regulation of the future internet and thus digitalization at large and that (b) provision, ownership, and operation relationships of infrastructure are increasingly complex.

Open RAN

The O-RAN Alliance is a group of network operators and equipment vendors founded by AT&T, China Mobile, Deutsche Telekom, NTT Docomo, and Orange in 2018 with the stated intent of increasing interoperability, promoting vendor diversity, and creating a common pool of intellectual property around mobile communications standards – as the name suggests, particularly when it comes to the radio access network. O-RAN has emerged as a potential alternative to proprietary offerings by, e.g., Ericsson and Nokia.

In the context of national security, O-RAN has been hailed to reduce cross-border dependences, although the actual outcome between business-as-usual 5G and O-RAN will greatly depend on details in implementation. For example, the UK has been keen to promote O-RAN is a strategy to have a more diverse and competitive provider market; it has set an ambition to have 35% of the UK's network traffic to be carried over O-RAN architectures by 2030.

O-RAN is largely a network architecture paradigm. Its promised benefits are interoperability, flexibility, innovation, cost reduction, and openness. In principle, any number of "white box" providers can design and sell gear for it.

While O-RAN potentially addresses some security concerns, it also raises others. After an intervention by the EU,[21] security aspects are now more prominent in O-RAN.

O-RAN deployments and trial phases are taking place in the US and Japan and are starting in Europe with trial phases and pilot projects.

Security

5G security implies
- availability,
- confidentiality, and
- integrity

of infrastructure, content, and data.

Security is the fundamental regulatory objective and obligates to design, to construct, and to maintain an infrastructure in which communications are not compromised by internal or external threats and quality of service is maintained under viable scenarios.

Fulfilling the objective necessitates identifying infrastructure and content elements, threat trajectories and vulnerabilities, and possible impacts of security lapses and their mitigation. Cybersecurity risks can be reduced but they cannot be removed altogether.

At the EU level, a key legislative piece in cybersecurity is the development of the EU 5G Toolbox and the revised NIS2 Directive (the European Network and Information Security Directive) which entered into force in January 2023, with the transposition deadline in October 2024.[22] NIS2 establishes a set of cybersecurity precautions and obligations to service providers as well as defines risk and security concepts and minimum measures to prevent incidences and to manage crises. It necessitates changes in the Member States' national security legislation.

Also, a relevant regulation is the Critical Entities Resilience Directive (CER), which also entered into force in January 2023.[23] The Commission has adopted a list of essential services in the eleven sectors and one of them is digital infrastructure, with services such as the provision and operation of internet exchange point service, domain name system, top-level domain, cloud computing and data center. Next the Member States have to identify the critical entities by July 2026. Once identified, the critical entities will have to take measures to enhance their resilience.[24]

The software-defined nature of 5G is both an asset and a liability when it comes to cybersecurity. Arguably, as compared to 4G, attack vectors should be fewer and more manageable. Operators nevertheless face new challenges in the 5G era:
- Multi-access edge computing requires mitigating data breach risk between operators' and enterprises' networks.
- With network slicing, tenants in a network must be strongly isolated with strict access control and end-to-end encryption.
- With higher bandwidth connectivity, malicious traffic, such as Distributed Denial of Service Attacks (DDoS), can become more vicious.
- Security management must become centralized and mostly automated.

While providers must be able to guarantee gear that is anomaly-resistant and vulnerability-free, in designing the system this aspect cannot be trusted.

As in any cloud computing application, 5G infrastructure is designed for seamless operation in case of hardware failure or misbehavior. Relatedly, the state-of-the-art in the ICT industry has long ago moved beyond security based on trusted brands and firewalls – the currently employed Zero Trust model assumes security breaches in a network and thus verifies each data request.

The idea of end-to-end (E2E) encryption is to protect data – in the context of 5G, voice, text, binary coded information, and metadata (e.g., caller records) – in transit and storage by making it unreadable if accessed by anyone but the sender and the intended receiver(s). When E2E is applied, the 5G infrastructure has no way to access the content of traffic it carries.

In cybersecurity, a chain is truly as strong as its weakest link; even though thinking of cybersecurity as an issue

spanning the whole infrastructure is cumbersome, little else makes practical sense. Cybersecurity must be holistic and coordinated to serve its purpose. It is important to attend to the entire lifespan of the network starting from its founding legislation and construction considering also critical equipment's' design, development, and procurement as well as implementation, operation, and maintenance.

The European Cybersecurity Agency ENISA conducted a deep dive into threats and risks in its Threat Landscape for 5G Networks report. As stated in the introduction to the report, "to better understand the cyber-threats affecting 5G Networks, it is essential to know the vulnerabilities and weaknesses of assets, assessing thus their attack surface and how it can be exploited by malicious actors." [25]

A more recent EU risk assessment was done on the cybersecurity and resilience of Europe's telecommunications and electricity sectors in July 2024. The risk evaluation identified both technical and non-technical risks such as the risks to the supply chain security, the lack of cyber professionals, and the risks posed by malicious activities from cyber criminals and state-sponsored threat actors. Supply chain risks were the main concern regarding 5G rollout. Also, ransomware, data wipers and exploitation of zero-day vulnerabilities were identified as ongoing risks. In addition, the physical sabotage of cable infrastructure and the jamming of satellite signals were identified as specific risks that are particularly difficult to mitigate.[26]

On the US side, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) has launched a 5G Cybersecurity project. As 5G becomes more widely available, operators and users of these systems must safeguard the technology from cyberattacks as 5G development, deployment, and usage evolves.[27]

ENISA is preparing a new candidate cybersecurity certification scheme for 5G. This work is based on the EU toolbox for 5G security and is expected to enhance the cybersecurity of 5G networks as part of a broader risk mitigation strategy. In this work ENISA is supported by the Ad Hoc Working Group. [28]

8 Regulation in the EU

Secure, resilient, performant, and sustainable digital infrastructures is one of the targets of Europe's Digital Decade Policy Programme 2030, which continues to steer the work of the EU and the new European Commission.[29]

The Commission acknowledges that the EU connectivity infrastructure is not yet ready to address the current and future challenges of the data-driven economy and the end-user needs. Faster and more secure connections are needed for deploying AI. This is expected to be addressed in the foreseen Digital Networks Act incentivizing the development of the digital networks of the future. [30]

The complex digital infrastructure ecosystem is regulated with a fragmented set of regulations. The Draghi report identified this inconsistency and restrictiveness of regulation as one of the reasons hindering Europe to close its innovation gap. The EU is behind its 2030 Digital Decade targets for fiber and 5G deployment.[31]

The aim of the 2018 European Electronic Communications Code was to promote connectivity by putting in place a regulatory framework to drive investments in high-capacity networks, and to cut red tape. However, the Commission does not deem the results to be satisfactory due to the delayed transposition by several Member States, but also because of the complexity of the framework and its procedures.[32]

The EU does not have a single market for digital communication networks and services, but 27 national markets with different supply and demand conditions, network architectures, and spectrum allocation procedures – regulation is only partly harmonized. The fragmentation concerns not only the supply side but also the demand side of the market. Radio spectrum policy is an area of shared competence between the EU and the Member States. There are also other national rules impairing the full realization of the Single Market, for instance, on lawful interception, data retention, and data localization rules.[33]

The recent geopolitical developments have highlighted the importance of security and resilience of key enabling technologies and critical infrastructures. There is a heightened need to rely on trusted suppliers and to mit-

igate vulnerabilities and dependencies. The EU 5G Cybersecurity Toolbox proposed a set of measures to mitigate the risks to 5G networks, to assess the risk profile of suppliers and exclusion of high-risk suppliers from the critical assets.[34]

The EU has passed two key legislative frameworks to enhance the security and resilience of the critical infrastructure, namely NIS2 and CER directives. Another recent addition is the Cyber Resilience Act, which places security-by-design obligations on the manufacturers of hardware and software products for their life cycle. The EU has also analyzed the cybersecurity implications of Open Radio Access Networks (RAN) to prepare for this paradigm shift of open interfaces in the 5G RAN architecture.

One reason for the slow 5G roll-out in the EU is the lack of coordinated and harmonized radio spectrum policy on the European level. Sufficient and efficiently used spectrum resources are needed for deployment of new wireless services for IoT, vertical use cases, and – in the future – 6G. The Draghi report calls for EU-level approaches to harmonize EU-wide spectrum licensing rules and processes.[35]

There are also EU funding instruments and programs that should be fully utilized to foster investment and to create new innovations in digital communication applications. As the Commission has assessed, massive investments in connectivity capacity are required to support the creation of a collaborative connectivity and computing ecosystem in Europe. The new Commission is planning to set up a new European Competitiveness Fund to foster investments in strategic technologies.

Protecting European interests and its critical infrastructures and communication networks calls for enhanced preparedness. Preparedness is an attitude, a mindset, but also a matter of credibility as extensively discussed in the Niinistö report. The foreseen Preparedness Union Strategy is foreseen to address the digital infrastructure needs as well.[36]

Key policies and legislation

While still incomplete, the EU has established a comprehensive regulatory framework to support the development and deployment of 5G. These policies and regulations aim to facilitate innovation, manage radio spectrum, and enhance cybersecurity. Key pieces of the EU's 5G policy and legislation are summarized in Exhibit 14.

In early 2013, the EU formed the 5G Public-Private Partnership (5G-PPP),[37] which aimed to boost 5G research and innovation.

Later efforts, including the 2016 5G Action Plan[38] and the 2021 Digital Compass,[39] provide milestones for achieving extensive 5G coverage across Europe, from urban areas to transport routes, with an ambitious target to reach all populated areas by 2030. These policies underscore the EU's commitment to staying competitive in the global digital landscape.

The State of the Digital Decade 2024 Report[40] provides an annual overview of the EU's progress towards achieving the 2030 targets set out in the Digital Decade Policy Programme. It tracks advancements across digital infrastructure, businesses, digital skills, and public services. It includes specific recommendations for the Member States. The report also details national strategic roadmaps submitted by the Member States and the European Commission's recommendations to address identified shortcomings. Some findings of the report include the need of the Member States to drive gigabit internet adoption to meet infrastructure targets and expedite the deployment of standalone 5G networks for full 5G potential. It is critical to thoroughly implement the 5G cybersecurity toolbox for secure networks. Supporting innovative digital solutions, especially among SMEs, is essential for economic growth. Significant EU investments underscore the importance of digital transformation in Europe.

Each regulatory piece has specific objectives to facilitate the 5G transition. For instance, the Radio Spectrum Policy Program (RSPP)[41] seeks to harmonize spectrum use across borders, making it easier for 5G networks to operate efficiently within the single market.

The European Electronic Communications Code (EECC)[42] was introduced to modernize telecommunications regulation, to simplify spectrum management, and to enhance data security provisions, which are essential for stable 5G connectivity. Complementary measures, such as the 2020 regulation on small-area wireless access

points, streamline the deployment of essential 5G infrastructure, particularly in dense urban areas.

Together, these policies and regulations (cf. Exhibit 14) create a multi-faceted approach aiming to ensure that the EU stays at the forefront of 5G innovation and maintains its geoeconomic influence by setting high standards for 5G governance and infrastructure in the global market.

9 Regulation in Finland

Of the recent legislative pieces, the EU 5G Toolbox is perhaps the most important one. It was explicitly designed to address geopolitical and geoeconomic concerns. However, since it left considerable leeway for interpretation, the Member States have implemented it quite differently. For example, Estonian and Sweden banned Chinese gear in their national infrastructures. Finland took a different route.

On 7 December 2020, The Parliament of Finland (Eduskunta) approved a law allowing authorities to ban telecommunications network equipment on grounds of a serious endanger to national security or defense.[43] The law introduces a new advisory board for monitoring security. It consists of representatives of the industry and the central authorities from different administrative branches. It discusses security and issues recommendations.

Unlike several other countries implementing the EU 5G toolbox, Finland neither banned vendors based on the country of origin nor singled out any. The Finnish law only applies to the most critical parts of the network – understood as the most central nodes of network traffic. The law also states that – if the authority orders network gear to be removed – the government will pay compensation.

The Finnish Transport and Communications Agency Traficom oversees defining practical elements relevant to the law and its enforcement. The advisory board for network security (Verkkoturvallisuuden neuvottelukunta) plays a key role in defining and designing the methods and process to implement the law with the contribution from the relevant ministries, authorities and the telecom operators and their industry association.

Exhibit 14 5G-related EU policies and legislation

EU Policy / Initiative	Description	Implications	Additional Info
5G Public-Private Partnership (5G PPP) (2013)	Public-private partnership for research and innovation in 5G technology.	Supports EU leadership in 5G innovation.	Part of a broader international strategy for global 5G consensus.
5G Action Plan (2016)	Early rollout of 5G infrastructure across Europe.	Aimed for 5G services in all Member States by 2020, 5G coverage in urban areas & transport routes by 2025.	Focuses on creating universal and continuous 5G coverage.
5G Toolbox (2020)	A set of measures for mitigating cybersecurity risks in 5G networks, ensuring secure deployment across Member States.	Strengthens security requirements for network operators, assesses supplier risks and diversification strategies.	Prepared by NIS Cooperation Group with support from European Commission and European Union Agency for Cyber Security (ENISA).
Digital Decade Policy Programme (2021)	Pathway to Europe's digital transformation by 2030 under the 2030 Digital Compass.	5G coverage for all populated areas and main transport paths by 2030.	A second assessment of the implementation of the digital principles provided in the 2024 State of the Digital Decade report.

EU legislation	Description	Implications
European Electronic Communications Code (EECC) (Directive (EU) 2018/1972)	**Telecommunications regulatory framework**. Consolidates and updates the regulatory framework for electronic communications, focusing on promoting high-speed networks like 5G by ensuring efficient and harmonized spectrum management.	Supports 5G rollout with improved spectrum coordination, stabilizes regulatory framework, promotes digital economy participation.
Radio Spectrum Policy Programme (RSPP) (Decision No 243/2012/EU)	**Management and harmonization of radio spectrum**. Sets policy goals and principles for managing radio spectrum within the EU's internal market, crucial for the harmonization and efficient use of 5G spectrum bands.	Facilitates harmonized spectrum allocation and usage across the EU, enhancing spectrum efficiency, transparency, and competition.
NIS 2 Directive (Directive (EU) 2022/2555)	**Updated cybersecurity rules addressing digitization and evolving threat landscape**. Updates the original NIS Directive (2016) by expanding its scope to new sectors and enhancing the cyber resilience of both public and private organizations, including telecom infrastructure.	Increases resilience and cybersecurity capabilities, covering more sectors and enhancing response measures to cyber threats.
Cyber Resilience Act (CRA)	The **new law** (adopted by the Council on 10 October 2024) introduces EU-wide cybersecurity requirements for hardware and software products, aiming to streamline regulations across EU member states and ensure high safety and environmental protection standard.	Stricter security standards for product lifecycles, helping secure EU's digital ecosystem and fostering cybersecurity from the ground up.
EU Cybersecurity Act (Regulation (EU) 2019/881)	Strengthens the mandate of ENISA and establishes a cybersecurity certification framework for ICT products, essential for securing 5G devices and systems.	Ensures high cybersecurity standards with certification of ICT products and services, reinforcing trust in 5G networks.
Small-area Wireless Access Points Regulation (Implementing regulation required by Article 57(2) of EECC)	Simplifies the deployment of small-area wireless access points for 5G networks, necessary for rapid and dense network infrastructure development.	Enables rapid installation of 5G small cells under simplified permit rules, supporting widespread deployment.
Digital Networks Act (DNA) Proposal	Proposed EU legislation aimed at redefining the EU telecoms regulation to ensure the development of cutting-edge digital network infrastructure.	Future-oriented piece of regulation proposed by the European Commissioner for Internal Market to redefine the EU's approach to regulating digital markets.

Source: A compilation by the authors.

10 Conclusions

Global economic progress over three decades up until around 2007 was largely based on increasing openness and on moderating political tensions and ideological differences. Recently geopolitics, as opposed to technology issues or market competition, have become the primary driver of developments in mobile communications. Major countries and blocs seek technological sovereignty but, in the case of technologically advanced products, they are still utterly dependent on geographically dispersed global supply chains.

Developments in 5G raise questions with respect to the future of free trade especially when it comes to technology intensive industries. Governments obviously have a legitimate interest in regulating the construction and use of 5G to safeguard national interests. Given the increasing prominence of mobile communications in the future, such public interests are likely to become increasingly pronounced.

As compared to 1G to 4G, 5G is a major technical and business discontinuity. The 5G is the first generation to fully embrace cloud computing principles and software defined networks (and virtualization, slicing, and verticals that come with it). It is also the first generation with a truly multi-band radio interface and reasonable integration with other over-the-air and wireline digital communications (although this aspect will be further deepened with the upcoming 6G). However, 5G's technical and business discontinuity also induces a regulatory discontinuity, which has not yet been fully addressed.

Endnotes

1 Amano Tatsushi is Director General of the Strategic Research Department at JBIC, Japan Bank for International Cooperation.

2 JBIC Today, Issue 2 February 2023: https://www.jbic.go.jp/en/information/today/today-2022/image/jtd_202302.pdf

3 The formal definition of geoeconomics by Wigell et al. (2022, p. 35) is as follows: "Government measures aimed at specific industries for strategic or national security reasons with the goal of protecting them at national level and/or harming those industries in a rival nation. Typical measures include financial sanctions; import bans; export bans; outward investment bans; inward investment screening; anti-competitive uses of product or market regulations, standards or administrative requirements; and state-sponsored industrial espionage and intellectual property theft."

4 As the example of North Korea suggests, division of labor and specialization, and associated economies of scale and scope, are so fundamental to human prosperity that such a deed would cause standards of living world over to collapse.

5 National interests may still be reasonably aligned with the domestic tech sector, albeit perhaps not to the extent Finland's interests were aligned with those of Nokia in the mobile telephony boom years.

6 https://www.act.nato.int/activities/next-generation-networks/

7 In 2024 according to https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/

8 http://www.economist.com/node/21560867

9 https://www.vinnova.se/en/publikationer/small-and-beautiful/

10 Establishing GSM was largely a meritocracy, in which the best technical solution would form the basis of a shared standard, which favored the two Nordic champions.

11 While some of the same functionality could be achieved with a dense mesh Wi-Fi, 5G is superior even within a narrowly defined location and a Wi-Fi based solution would typically not be feasible, if either the geographical span extends or a transfer of network traffic from private to public infrastructure is called for.

12 Drives & Controls (First private 5G industrial network is set up in Germany, 3 January 2020): https://drivesncontrols.com/first-private-5g-industrial-network-is-set-up-in-germany/

13 Accenture Strategy, February 2021: The Impact of 5G on the European Economy (A study commissioned by Qualcomm and conducted by Accenture). https://www.accenture.com/_acnmedia/PDF-144/Accenture-5G-WP-EU-Feb26.pdf

14 5G will always have multiple physical touchpoints.

15 For example, in autonomous vehicles, the heaviest lifting will happen within a vehicle over wires, but information exchange with other vehicles (say, a warning of an emergency braking) can only happen over-the-air. In the context of 5G, edge computing will often take place at the base station to which the device is connected – from a few meters to a few kilometers from the point of use. It is not the case that all applications need the maximum speed and the minimum response time. Consider a tracking device such as Apple's AirTag (Although we should point out that the functionality of Apple AirTag is based on near-by Apple devices, not directly on mobile telecom infrastructure.). For practical purposes, latency is irrelevant; a response time of a few seconds is fine (a few seconds in computing is something approaching infinity). The need for bandwidth is minuscule (a relevant data transfer basically includes the coordinates and an on/off signal for ringing or similar functionality; this data volume rounds to nil in today's world). For a tracking device, the network's key features are (a) an extensive geographical coverage (including passing any physical obstacles and thus, e.g., finding your stuff in a bomb shelter or at the bottom of a lake) and (b) a low power consumption (ideally, years of connectivity of a small device without a battery change or charge).

16 Formal requirements of 5G have been defined under the United Nations' specialized agency for ICT, the International Telecommunication Union (ITU-R Working 5G Party 5D). As compared to 4G, 5G should deliver tenfold actual user-experienced data rates, one tenth of the latency, and ten times the number of connections per square kilometer. And all this with one hundredth of energy used per bit transferred (bits per joule) and three times the spectrum efficiency (bits per second per hertz).

17 One of the still bending concerns is that net neutrality regulations hamper network slicing and hinder differentiation across customers.

18 Enrique Duarte Melo, Val Elbert, Antonio Varas, Heinz Bernold, and Helen Kondos, September 2020: Building the US 5G Economy. Boston Consulting Group in collaboration with CTIA. https://web-assets.bcg.com/a1/ce/a94e590d46ee8712aed2e9eb4057/bcg-building-the-5g-us-economy-sep-2020-r.pdf

19 5G and Future Connectivity: An Emerging Framework for Irish Cities and Towns (discussion document). https://smartdocklands.ie/5G

20 5G-PPP, Infrastructure 5G Innovations for New Business Opportunities (Brochure), 2017, p. 3, https://5g-ppp.eu/wp-content/uploads/2017/03/5GPPP-brochure-final-web1-with-Author-credits.pdf

21 Report on the cybersecurity of Open RAN", NIS Cooperation Group, the European Union, 11 May 2022, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks

22 https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

23 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992

24 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992

25 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

26 https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors. The risk assessment report was based on the February 2024 report on the cybersecurity and resilience of the EU communications infrastructures and networks: https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks

27 https://www.nccoe.nist.gov/sites/default/files/2023-01/5g-cybersecurity-fact-sheet.pdf

28 https://www.enisa.europa.eu/topics/certification/copy_of_adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification

29 The European Commission White Paper "How to master Europe's digital infrastructure needs? COM(2024) 81 final, 21.2.2024, p 6. https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

30 The European Commission White Paper "How to master Europe's digital infrastructure needs? COM(2024) 81 final, 21.2.2024, p 6. https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs. Commissioner-designate Henna Virkkunen, Mission letter, 17.9.2024 https://commission.europa.eu/document/3b537594-9264-4249-a912-5b102b7b49a3_en

31 The future of European competitiveness: Report by Mario Draghi, 9.9.2024 https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en#paragraph_47059

32 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018.

33 The European Commission White Paper "How to master Europe's digital infrastructure needs? COM(2024) 81 final, 21.2.2024, p 13.

[34] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, 23 January 2020 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[35] The future of European competitiveness: Report by Mario Draghi, 9.9.2024

[36] Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness Report by Sauli Niinistö, former President of the Republic of Finland, In his capacity as Special Adviser to the President of the European Commission, 30.10.2024. Europe's Choice Political Guidelines for the Next European Commission 2024-2029, Ursula von der Leyen Candidate for the European Commission President, 18.7.2024

[37] https://5g-ppp.eu/

[38] https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan

[39] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

[40] https://digital-strategy.ec.europa.eu/en/factpages/state-digital-decade-2024-report

[41] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02012D0243-20201221

[42] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20241018

[43] https://finlex.fi/fi/esitykset/he/2020/20200098

Literature

Ali-Yrkkö, J., Kuusela, O.-P., & Kuusi, T. (2024). Geopolitiikka muuttaa maailman taloutta. *Etla Raportit nro 150*. https://pub.etla.fi/ETLA-Raportit-Reports-150.pdf

Fransman, M. (2010). *The new ICT ecosystem: implications for policy and regulation / Martin Fransman*. Cambridge University Press. https://doi.org/10.1017/CBO9780511676130

Hannah, D., & Eisenhardt, K. (2018). How firms navigate cooperation and competition in nascent ecosystems. *Strategic Management Journal*, *39*(12), 3163–3192. https://doi.org/10.1002/smj.2750

Harakka, T. (2023). *Data Capitalism in a World of Crises*. Siltala Publishing. https://timoharakka.fi/wp-content/uploads/2023/06/Timo-Harakka-Data-capitalism-in-the-world-of-crises.pdf

Hoeschele, T., Dietzel, C., Kopp, D., Fitzek, F., & Reisslein, M. (2021). Importance of Internet Exchange Point (IXP) infrastructure for 5G: Estimating the impact of 5G use cases. *Telecommunications Policy*, *45*(3), 102091. https://doi.org/10.1016/j.telpol.2020.102091

Normann, R. (2001). *Reframing Business: When the Map Changes the Landscape*. John Wiley & Sons. https://archive.org/details/isbn_9780471485575

NTT DOCOMO (2022). 5G Evolution and 6G. *White Paper*, *January 2023* (Version 5.0). https://www.docomo.ne.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_v5.0.pdf

Suraci, C., Araniti, G., Abrardo, A., Bianchi, G., & Iera, A. (2021). A stakeholder-oriented security analysis in virtualized 5G cellular networks. *Computer Networks*, *184*, 107604. https://doi.org/10.1016/j.comnet.2020.107604

Thorén, K. (2021). How digital platforms transform industries. In V. Long & M. Holmén (Eds.), *Technological Change and Industrial Transformation* (pp. 47–73). Routledge. https://doi.org/10.4324/9780429423550

Valkokari, K. (2015). Business, innovation, and knowledge ecosystems: How they differ and how to survive and thrive within them. *Technology Innovation Management Review*, *5*(8), 17–24. http://timreview.ca/article/919

Wigell, M., Borchert, H., Christie, E., Fjäder, C., & Hartwig, L.-H. (2022). Navigating geoeconomic risks: Towards an international business risk and resilience monitor. *FIIA Reports*, *71*. https://www.fiia.fi/en/publication/navigating-geoeconomic-risks

Yan, X., & Huang, M. (2022). Leveraging university research within the context of open innovation: The case of Huawei. *Telecommunications Policy*, *46*(2), 101956. https://doi.org/10.1016/j.telpol.2020.101956

ETLA

Elinkeinoelämän tutkimuslaitos

ETLA Economic Research

ISSN-L 2323-2447,
ISSN 2323-2447,
ISSN 2323-2455 (Pdf)

Kustantaja: Taloustieto Oy

Puh. 09-609 900
www.etla.fi
etunimi.sukunimi@etla.fi

Arkadiankatu 23 B
00100 Helsinki