The challenge of 5G security

Brought to you by Informa Tech

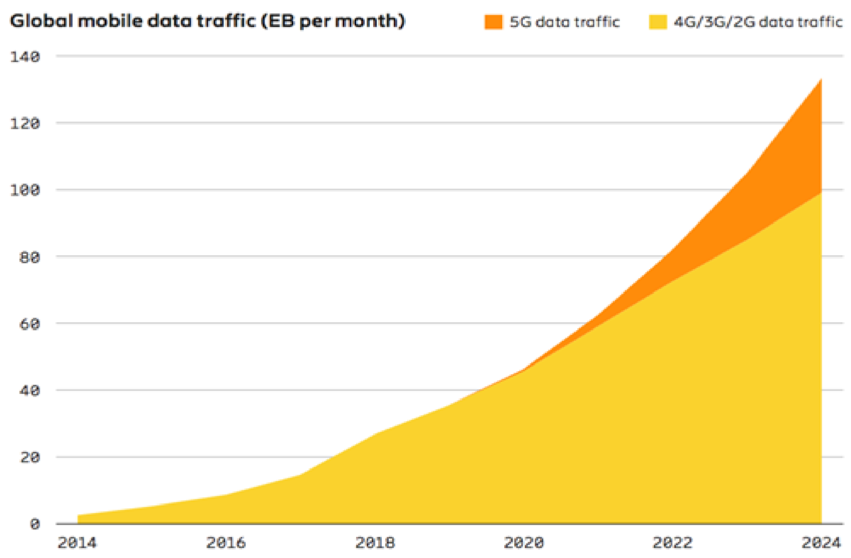
Contents

Introduction

While the global consumer 5G market is still in the early stages of development, operator commitment to network rollouts in 2019, in tandem with highly competitive pricing approaches, has secured a solid foundation for subscription growth acceleration in 2020. Aside from coverage and pricing, devices are of course key to how quickly a new technology gets taken up, and growing commitment among manufacturers to include 5G in a broader range of devices also ensures that mass-market take-up of 5G will begin in earnest in 2020. True to form, Apple's 5G plans are currently only to be guessed at, but if it decides to include the technology in all of its 2020 iPhones, then 4Q20 will mark a major inflection point for consumer 5G.

Meanwhile, operators are actively forming partnerships to explore the benefits of a huge range of 5G enterprise and industrial use cases, and while these are understandably taking longer to put in place, their potential to transform industries is immense. Indeed, one major and fundamental difference between 4G and 5G that 2020 may start to uncover is that the new technology is far more transformative for the enterprise and industrial markets (the connected digitization of an immense range of processes for the first time) than it is for consumer (faster speeds and more data). One of the key remaining questions for 5G rollouts and adoption is how providers will implement 3GPP security for 5G networks, and what additional security controls and technologies will need to be put in place to ensure privacy and availability, especially considering the new enterprise and industrial applications of 5G.

Exhibit 1: 4G and 5G mobile traffic



Source: Omdia 2020

Key messages

- **So far, 5G's new capabilities are few – but, as with 4G, that's enough to spark consumer interest.** For the end-user, 5G at launch is simply 4G, only better. But faster speeds, greater immediacy (through lower latency), and more value (data, content, or both) are enough for consumers to move to a new technology when the network delivers an improved experience. There is also some expectation of increased security with 5G compared to 4G, as consumers generally expect security to improve in new generations of all technology. However, most consumers are unlikely to pay a significant premium for 5G, either in terms of device or price plan cost, because of limited 5G network coverage, and because LTE/LTE-A already gives an excellent experience for all but the most tech-demanding of users.

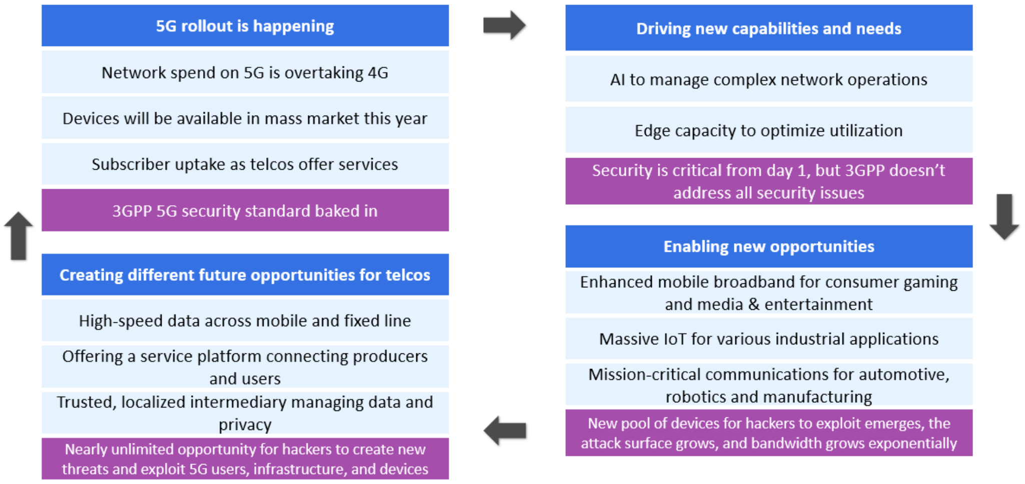
- **If 5G is a race, it's a marathon, not a sprint.** First-mover advantage is there only if an operator continues to increase coverage. Omdia’s research showed that operators which didn't launch 4G first, but which expanded network coverage rapidly after launch, can overtake first-movers that rushed to launch and then didn't rapidly expand coverage. Because of 5G's greater network complexity, this may be even more true than it was for 4G, as those that are later to market take advantage of network improvements – and at lower cost. We also advise that providers take both 3GPP security and additional security controls seriously earlier in the deployment process.

- **In 2020, 5G's benefits will start to be felt in earnest on enterprise and vertical markets.** As leading service providers build-out 5G network coverage in tandem with broader network transformation they will be in a strong position to offer enterprise and vertical markets connected mobility services that 5G's increased performance in terms of capacity and latency will make possible for the first time. Network operators that can demonstrate market-leading network and service delivery capability, and those that choose the best partners to do so with, will be in a strong position to take advantage of the new connected mobility opportunities 5G opens. Network operators that deploy robust security solutions for their own infrastructure, and new security services for both consumers and enterprises will also outmaneuver those who don’t.

Security and 5G

5G deployments are accelerating, and though the promises of 5G—new capabilities that enable a wide range of new uses/applications—are undeniable. The 3GPP security standard was well considered and developed, but it's a set of recommendations/requirements that still require service providers to select technology, configure and deploy it properly, and maintain vigilance, because 5G creates an infinite number of opportunities for hackers to develop attacks. Attacks will grow in bandwidth/scale and diversity, focus on the seams between connection points in networks (and between 4G and 5G networks), and exploit newly connected IoT devices and the powerful new services they enable.

Exhibit 2: 5G enables new services and new attacks



5G rollout is happening

Network spend on 5G is overtaking 4G

Devices will be available in mass market this year

Subscriber uptake as telcos offer services

3GPP 5G security standard baked in

Driving new capabilities and needs

AI to manage complex network operations

Edge capacity to optimize utilization

Security is critical from day 1, but 3GPP doesn't address all security issues

Enabling new opportunities

Enhanced mobile broadband for consumer gaming and media & entertainment

Massive IoT for various industrial applications

Mission-critical communications for automotive, robotics and manufacturing

New pool of devices for hackers to exploit emerges, the attack surface grows, and bandwidth grows exponentially

Creating different future opportunities for telcos

High-speed data across mobile and fixed line

Offering a service platform connecting producers and users

Trusted, localized intermediary managing data and privacy

Nearly unlimited opportunity for hackers to create new threats and exploit 5G users, infrastructure, and devices

Source: Omdia 2020

Existing security requirements will not be enough to protect 5G networks from threats

5G networks will connect countless objects, including those in critical sectors. The greater reliance of economic and societal functions on these networks could significantly worsen the potential negative consequences of disruptions. Therefore, it is essential that any vulnerabilities in the networks are addressed sooner rather than later. By the end of 2020, the EU nations will have among the largest deployments of 5G across a diverse set of interconnected networks, so to stay ahead of the possible issues associated with 5G security, the EU produced a cybersecurity report in 2019. While this report focuses on the EU, the findings are relevant to the 5G industry globally. The report is based on the results of the national cybersecurity risk assessments conducted by member states, and identifies the main threats and threat actors affecting 5G networks, as well as the most sensitive assets.

The cybersecurity report highlights the main vulnerabilities related to the compromise of confidentiality, availability, and integrity, and it also looks at strategic risks. The assessment provides the basis on which the EC will identify mitigation measures that can be applied at both a national and EU level. Regulators have attempted to outline the most important threats, such as 5G network disruption, spying of traffic/data, modification or rerouting of traffic/data, and destruction or alteration of other digital infrastructures. The severity of specific threat scenarios to 5G networks varies according to a number of factors, including the number and type of users impacted; the length of time of the event before detection or remediation; the type of services impacted; the extent of damage; and the type of information breached.

According to the national risk assessments, threats posed by states or state-backed are perceived to be of highest relevance by member states. They represent the most serious as well as the most likely threat actors, because they have the motivation, intent, and the capability to conduct persistent and sophisticated attacks. Although the EU has so far resisted US pressure to boycott Chinese companies such as Huawei and ZTE, it seems likely that the results of these risk assessments will encourage the EC to look at addressing possible risks from non-EU state or state-backed actors.

The report has also identified a number of important security challenges that are likely to become more prominent in 5G networks; for example, the role of suppliers in building and operating 5G networks that results in greater access of third-party suppliers to networks and to interlinkages between 5G networks and third-party systems, as well as the degree of dependency on individual suppliers that increases the exposure to a potential supply interruption. The risk profile of individual suppliers will become particularly important, including the likelihood of the supplier being subject to interference from a non-EU country. Key innovations in the 5G technology, particularly the important part of software and the wide range of services and applications enabled by 5G, also pose challenges because these increase the number of potential entry points for attackers.

All these challenges create a new security paradigm, making it vital that regulators reassess the current policy and security framework. Existing security, data privacy, and protection requirements relevant to the 5G networks are set out in legislation around the globe. Many security measures may already be applied by MNOs, such as technical measures (e.g., encryption, authentication, automation, and anomaly detection) or process-related measures (e.g., vulnerability management, and incident and response planning). However, the fundamental differences in how 5G operates means that current security measures employed on 4G networks are not comprehensive enough to mitigate security risks.

Bottom line

5G rollouts are here, and your customers, partners, regulators, and hackers are all watching closely. Security for your network is more important than ever, and it needs to be a key consideration in all layers of the 5G rollout process, from design to operation. Service providers need to bake in security across their infrastructure--from the end device, through the edge and core, and back, as there are many potential points of entry that will be exploited. Comprehensive deployment at scale will require security embedded into wireless infrastructure, IP network infrastructure, and dedicated security solutions.

To learn more

Watch this free webinar

“Modernizing 5G infrastructure security”

presented by Omdia and our partners

JUNIPER NETWORKS ERICSSON

The webinar can be accessed at: https://bit.ly/2Uk6PyL

For additional Omdia events, visit:
https://technology.informa.com/Events

Follow the conversation @OmdiaHQ

Authors

Sarah McBride
Analyst, Service Providers

Jeff Wilson
Senior Research Director, Cybersecurity Technology

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.