Realising the potential of IoT in MENA

November 2019

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

GSMA Intelligence

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

Authors:
Mark Little, Senior Manager
Sylwia Kechiche, Principal Analyst
Yiru Zhong, Lead Analyst
Alex Gharibian, Forecast Analyst

Contributors:
Graham Trickey, Head of IoT
Jawad Abbassi, Head of MENA
Amr Hashem, Technology Director, MENA
Kenechi Okeleke, Senior Manager
Jade Nester, Director, Consumer Policy

CONTENTS

Executive summary

IoT connection growth in MENA second only to Asia-Pacific

IoT connections in the Middle East and North Africa (MENA) region are growing at a rate second only to Asia-Pacific. With a well-established smart city vision acting as a catalyst for the IoT market, initiatives from governments and the mobile industry are expected to be fundamental in helping IoT revenues reach $55 billion by 2025. The commitment to and innovation in IoT seen across MENA is also expected to benefit the GDP of the regional economy to the tune of $18 billion in 2025.

Operators need to move beyond connectivity to monetise IoT

The region's IoT ecosystem (which includes operators, IoT vendors, systems integrators and business customers) needs to exploit the synergies available from 5G-based IoT deployments to innovate, adopt and deploy new services. These include 'applications, platforms and services' – a category of IoT services expected to win a majority share of the market worth more than $30 billion by 2025. To take a greater share of the IoT revenue opportunity, operators need to move beyond connectivity into strategic partnerships with ecosystem players and even governments to launch new value-added services.

Governments play a pivotal role as policymakers and customers

Mobile operators and the ecosystem as a whole cannot gain traction without the vision and support of regional and national policymakers to develop the IoT market and capture the social, commercial and economic benefits available. Governments can play a pivotal role as both policymakers and customers, as they have their own digital transformation agendas. National governments can encourage IoT market growth through regulation (e.g. smart fire alarms) and by exploiting the power of IoT sensors and automation to enhance public services.

Strategic opportunity lies in integrating security and data protection in IoT

This report illustrates the market potential across MENA's IoT ecosystem and points to growth trends in smart cities, industrial IoT and consumer IoT. But it also recognises the challenges, with the biggest likely to be around security and data protection. The region has a strategic opportunity to lead on security by design and ensure cybersecurity and data protection are built in from the start. The GSMA and mobile industry have contributed to the security initiative by introducing the GSMA's IoT Security Guidelines and IoT Security Self-Assessment. This report includes examples of best practices from the global regulatory environment.

Mobile operators are vital to the success of IoT in the region

Mobile operators possess foundational assets and capabilities for targeting the IoT ecosystem in the form of 5G and NB-IoT networks, the power of the SIM, and key customer-facing channels and partnerships to help take IoT propositions to market. Operators are in the process of establishing these assets in the IoT ecosystem, making them vital to the success of IoT services in the region.

1 The MENA IoT market in context

The Internet of Things is a fast growing opportunity for mobile operators in the MENA region. By 2025, the region is forecast to account for around 4% of global IoT connections, growing at a CAGR of 16% – the second fastest regional growth rate after Asia Pacific.

In 2019, the consumer and industrial IoT segments have equal shares of total IoT connections, but industrial IoT is where most of the growth will occur, reaching 57%[1] of total connections by 2025, driven by an increase in smart utilities, smart retail and smart city deployments. Growth in connections will help drive IoT revenues, which are expected to grow at an annual rate of 19% to reach $55 billion[2] by 2025. Applications, platforms and services (a category that includes platforms, applications, cloud, data analytics and security) will show the strongest growth, at a CAGR of 23%. It will account for 55% of the region's IoT revenues by 2025.[3]

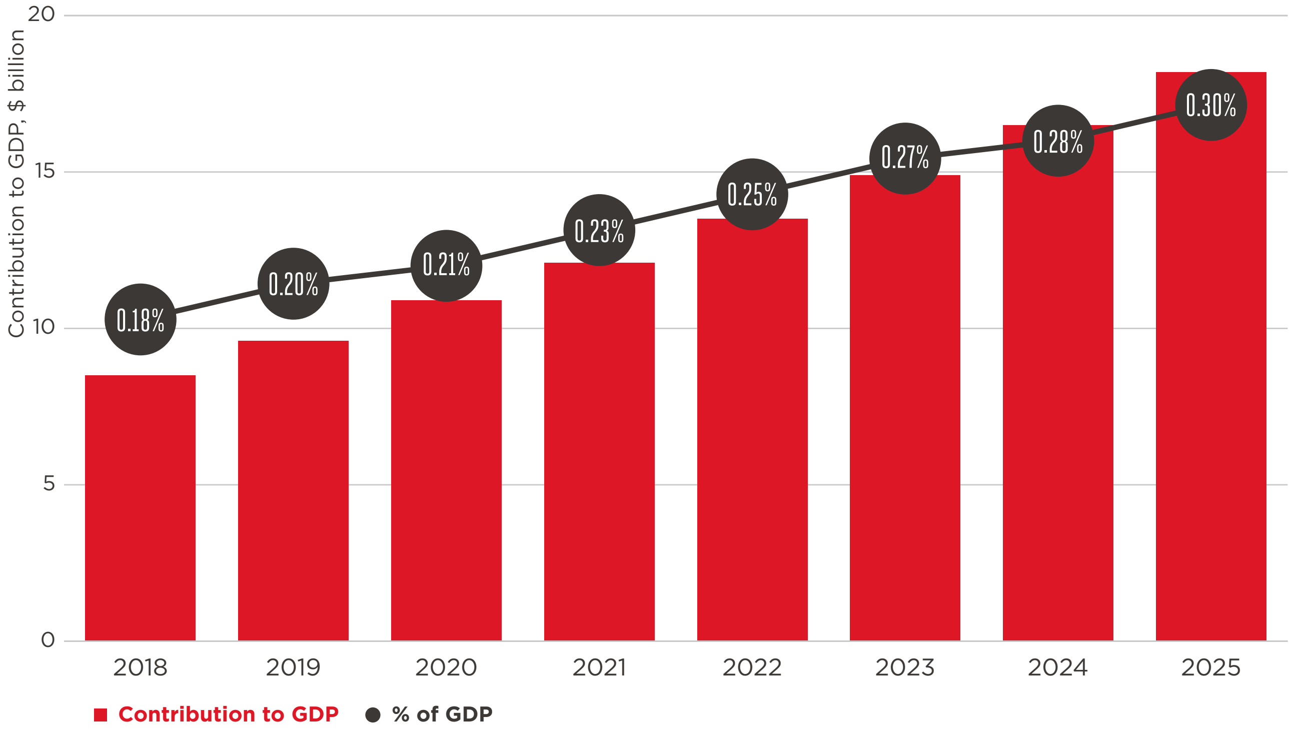
Although IoT in the region is still nascent, its share of global IoT revenues is approaching 6%, significantly ahead of its economic share of GDP, which is just under 4%. Strong growth in IoT connections, an early-adopter mindset and aggressive plans for smart cities make the region one of the world's most active IoT economies.

1.1 IoT contributes to the region's economic growth

The regional economy is expected to benefit from a productivity impact from the use of IoT-based products and services. Potential gains for businesses in developing countries, in general, are substantive; enterprises are already saving 4–5% of costs with a relatively low level of IoT deployment. The GSMA estimates the economic benefit to be $8.5 billion in 2018, rising to $18 billion in 2025, equivalent to a GDP contribution of 0.3% to the economy in MENA.

Figure 1

Productivity benefit from IoT in MENA



Source: GSMA Intelligence

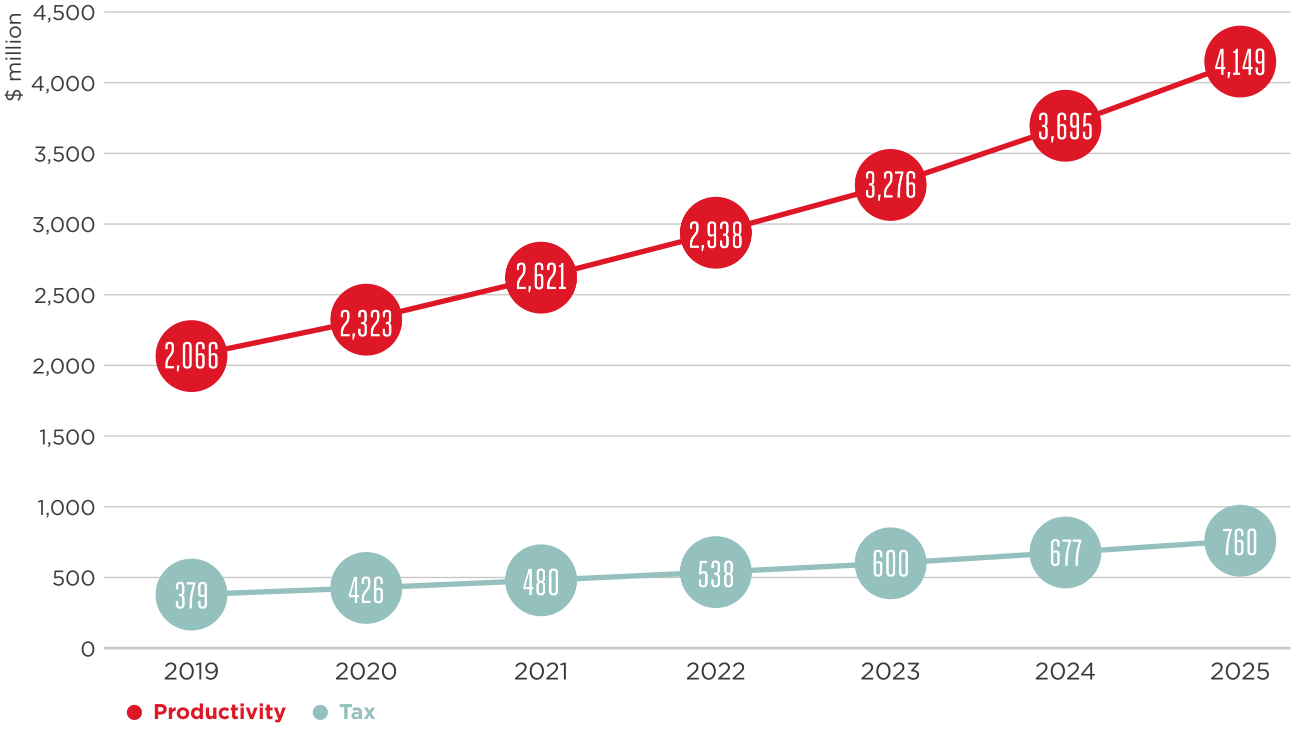
The deployment of IoT services and solutions could mitigate the slowdown in productivity growth currently experienced in both developed and developing economies. With half the economic benefit from IoT enjoyed by manufacturing businesses, it is even possible that IoT deployments could reverse the slowdown in productivity.

[1] GSMA Intelligence
[2] IoT: the $1 trillion revenue opportunity, GSMA Intelligence, 2018
[3] GSMA Intelligence

Governments are set to gain fiscally from the growth of IoT services. Productivity gains by the wider economy result in more government revenue as taxes are payable on the wider economy's corporate income, and sales in particular. Using Turkey as an example, we estimate that productivity gains in 2019 from IoT will contribute over $2 billion to government revenue in the country, rising to more than $4 billion by 2025 – and this does not include direct and indirect tax contributions from the IoT ecosystem.

Figure 2

Turkey: incremental productivity and tax contribution to GDP



Source: GSMA Intelligence

Globally, enterprises report savings of between 4% and 6% of operating costs, but developing countries are reporting higher cost savings than developed economies. In MENA, for example, Turkey reports nearly 6% cost savings, suggesting the region as a whole could experience similar above-average economic benefits from IoT adoption.

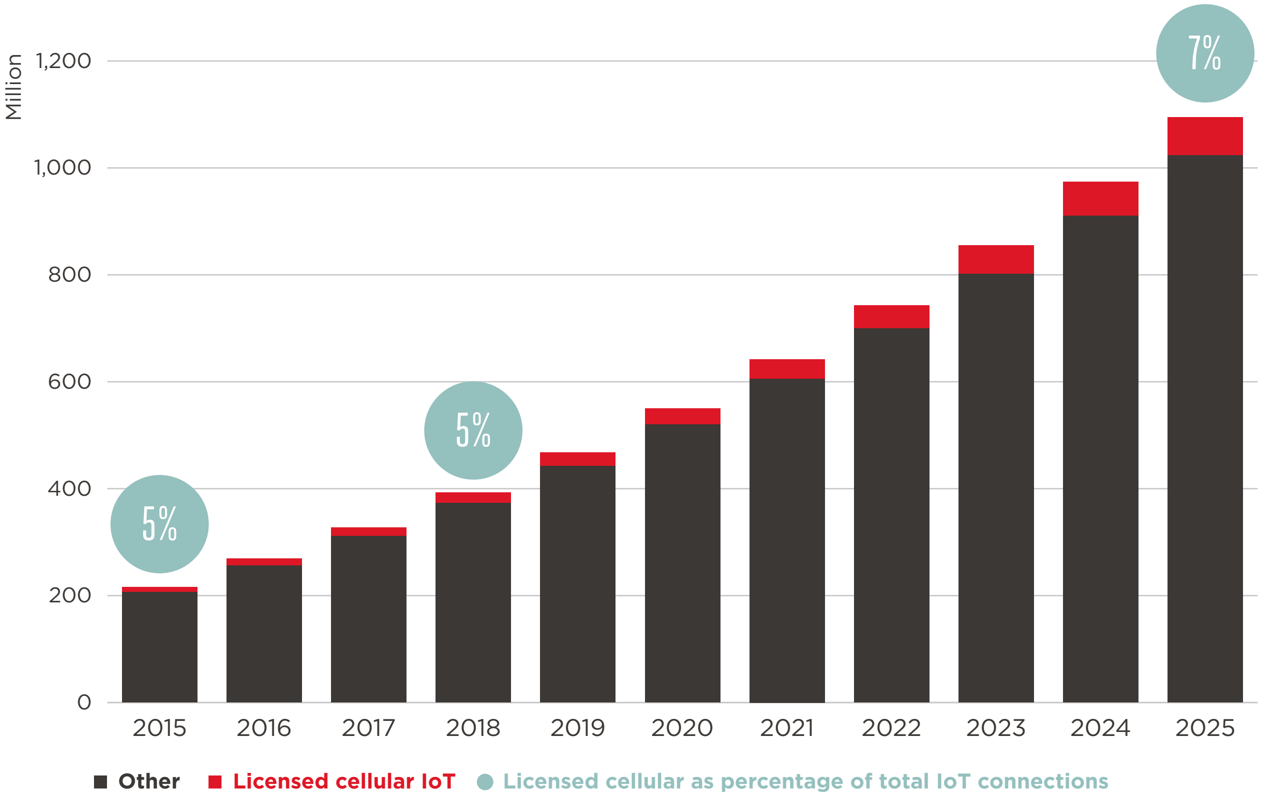
The GSMA Intelligence IoT Enterprise Survey 2018 indicates that the largest gains in cost savings are likely to occur when enterprises shift from deploying a minimal number of devices (less than 50) to deploying over 300 devices. This suggests that governments that focus on improving IoT adoption will yield significant growth in their tax receipts through improvements in enterprise productivity.

2 Key trends in the MENA IoT ecosystem

Growth in IoT adoption in MENA is being propelled by government efforts to address resource scarcity and improve the well-being of citizens. A drive by enterprises to improve efficiencies and reduce costs by using IoT solutions is also helping to spur connections. Between 2017 and 2025, IoT connections are expected to triple to reach 1.1 billion (see Figure 3).

Figure 3

IoT connections in MENA



Source: GSMA Intelligence

2.1 Connectivity mix and the role of operators

The majority of IoT devices – typically in indoor environments – will be connected by unlicensed radio technologies designed for short-range connectivity, such as Wi-Fi, Z-Wave and Zigbee. While operators naturally focus on their own networks, some also recognise the opportunity in unlicensed radio technologies and the customer overlap with their cellular network. Before the advent of Mobile IoT, several operators had invested in other unlicensed networks such as LoRa. For example, Ooredoo Oman partnered with Sagemcom and NEC to build a LoRa network to roll out smart metering for the National Electricity Centre (NEC). Meanwhile, its subsidiary, Ooredoo Tunisia, launched LoRa in 2018 to address opportunities in smart city, smart industry and smart environment.

However, IoT devices that require mobility, lower latency and ultra-reliability will primarily be connected by cellular networks using licensed spectrum. Mobile IoT refers to low power wide area (LPWA), 3GPP standardised, secure operator managed IoT networks in licensed spectrum – in particular, LPWA networks designed for IoT applications that are low cost, use low data rates, require long battery lives and often operate in remote, hard-to-reach locations. Cellular networks address the need for more secure, managed connectivity that can connect directly to the cloud (as opposed to the gateway or hub) and will be one of the key drivers of IoT growth across enterprises. Licensed cellular networks will serve 3.5 billion IoT connections globally by 2025 or 13% of the total number of IoT connections. In MENA, licenced cellular IoT accounted for 5% of total IoT connections in 2018; this will increase to 7% by 2025. The number of licensed cellular IoT connections in MENA will grow to more than 70 million by 2025.

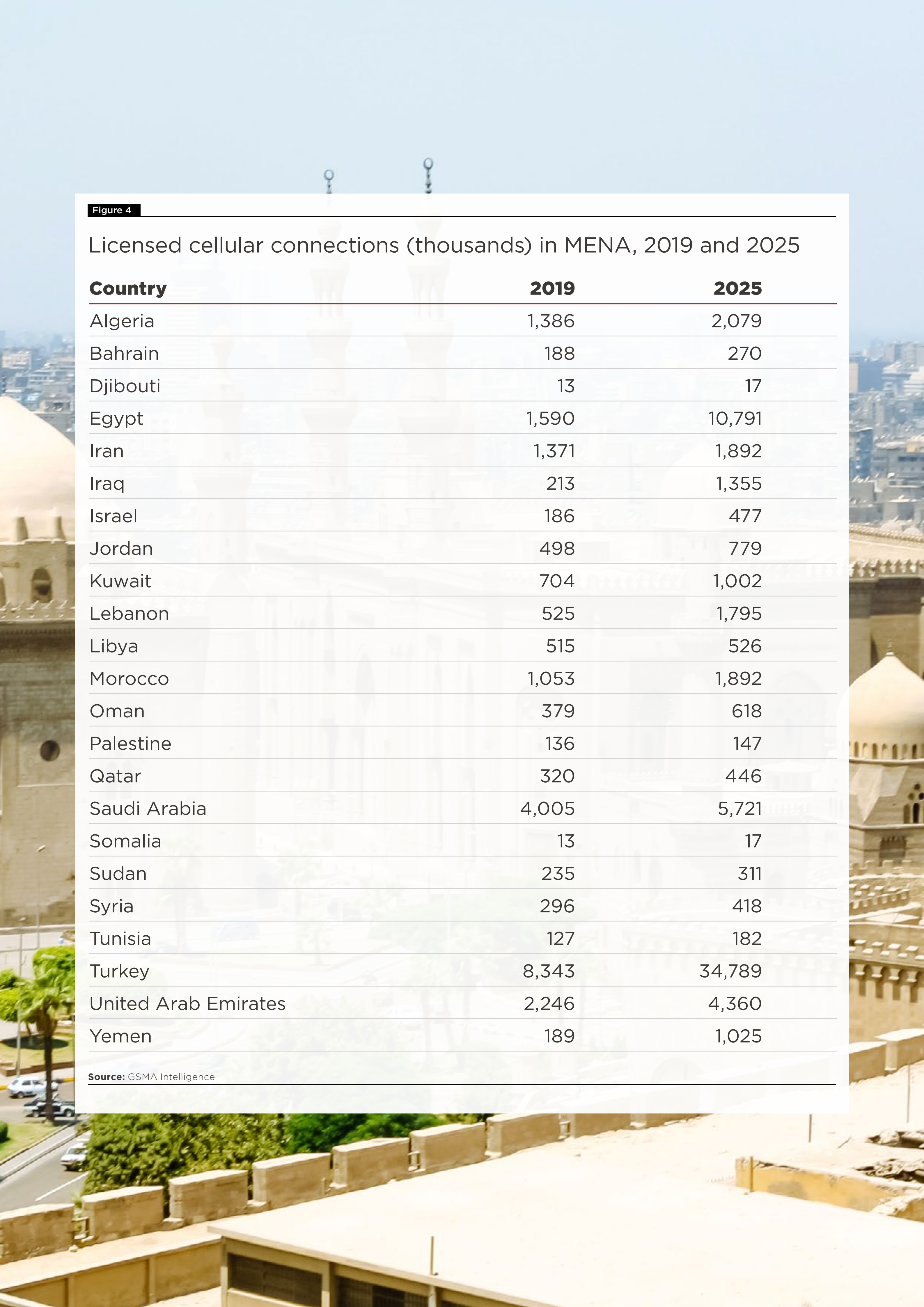


Figure 4

Licensed cellular connections (thousands) in MENA, 2019 and 2025

Country	2019	2025
Algeria	1,386	2,079
Bahrain	188	270
Djibouti	13	17
Egypt	1,590	10,791
Iran	1,371	1,892
Iraq	213	1,355
Israel	186	477
Jordan	498	779
Kuwait	704	1,002
Lebanon	525	1,795
Libya	515	526
Morocco	1,053	1,892
Oman	379	618
Palestine	136	147
Qatar	320	446
Saudi Arabia	4,005	5,721
Somalia	13	17
Sudan	235	311
Syria	296	418
Tunisia	127	182
Turkey	8,343	34,789
United Arab Emirates	2,246	4,360
Yemen	189	1,025

Source: GSMA Intelligence

NB-IoT and LTE-M in MENA: key developments

Mobile IoT networks enable the connection of IoT devices that require longer battery life and lower data throughputs. The technology also offers deeper indoor coverage, while retaining the security associated with cellular, and the ability to achieve global coverage due to its roaming capabilities. As of September 2019, there were 121 commercial launches of Mobile IoT globally across several countries, including the UAE, Saudi Arabia and Turkey.

Operators are deploying NB-IoT and LTE-M as a connectivity option for smart cities, utilities, retail and other verticals. Following trials with Huawei, in July 2017, UAE Etisalat launched NB-IoT and LTE-M networks. Du also launched NB-IoT in February 2019 based on the latest 3GPPP Release 14 standard, in partnership with Nokia, Affirmed Networks and MediaTek. The launch futureproofs Du's investment in massive IoT, enabling it to deliver applications such as smart metering, smart parking, vehicle trackers, smart health and agriculture.

Turkcell launched the country's first NB-IoT network in August 2017 and now provides LTE-M, offering connectivity for smart metering and smart city use cases such as parking and waste management. In November 2018, Turkcell introduced Turkcell Filiz, an NB-IoT device and mobile application enabling farmers to increase productivity through remote monitoring that offers a 10% saving on irrigation. It gives farmers access to data about their fields, disease management and climate conditions such as temperature and soil moisture thanks to agricultural sensor stations.

Vodafone Turkey followed suit, launching its NB-IoT network soon after for the same applications. In 2018, Turk Telekom launched its smart health initiative using NB-IoT. The operator's smart organ-carrying bag, developed in partnership with Borda Technology, Ankara Guven Hospital and Nokia, continuously measures and provides online reporting on a number of parameters such as temperature, humidity levels and lid movements.

In March 2018, STC chose Ericsson to expand its 4G network in Saudi Arabia including deployment of LTE-A (Advanced) and NB-IoT to support massive IoT applications such as smart metering and parking sensors.

2.2 Consumer IoT boosted by operator partnerships

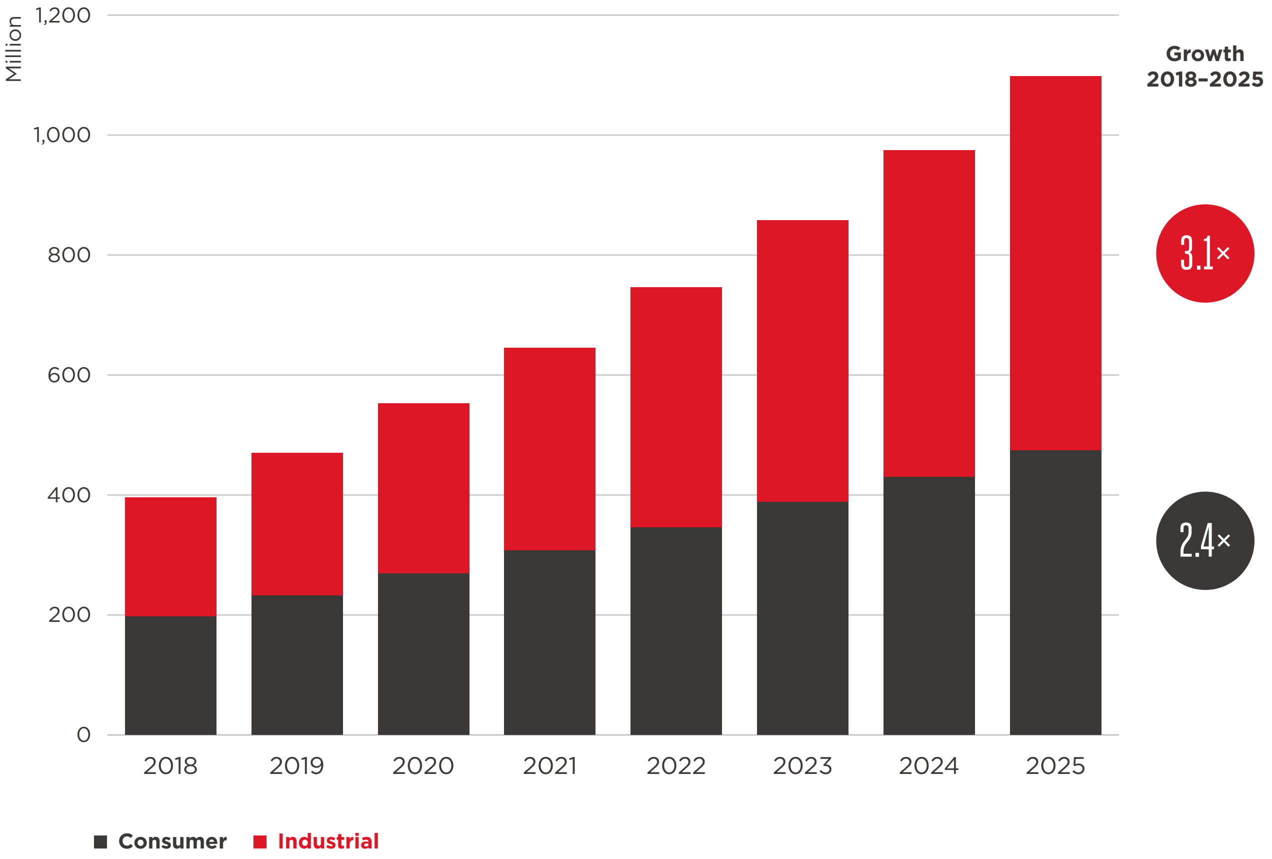
Until 2018, consumer IoT accounted for the majority of IoT connections in MENA, driven by adoption of smart home and home security systems. Partnerships have been an important route to market and are successfully driving adoption. For example, Hitches and Glitches (a home maintenance company) inked a partnership with Ring (a smart home security company) in August 2019 to install smart home security devices into residential communities in the UAE. Several city bicycle-sharing schemes also exist in the region including in Istanbul, Izmir, Abu Dhabi and Doha.

Operators are also offering IoT services to consumers:

- A year after the initial launch of its smart home offering, Zain Life, Zain Kuwait began offering smart home plans. These include home security and mesh networking devices to provide better indoor coverage.
- In August 2019, Vodafone Qatar announced its new smart home plan, GigaHome Smart, which includes smart plugs, window/door sensors and smart bulbs. It uses Vodafone's GigaHome platform – a home internet solution provided by Vodafone Qatar's GigaNet network including 5G and fibre.
- Du launched its smart home services in the UAE in 2017 focused on home automation, monitoring and entertainment. The operator has collaborated with Somfy, Schneider Electric and Ring, among others. Du offers three packages: a tailor-made "Custom Solution", a ready-to-go "Bundle Solution" and a "Plug & Play" solution that can be used straight out of the box.
- Maroc Telecom was the first operator in North Africa to launch a smart home offering in December 2015, in partnership with Somfy. The operator has expanded its offering to include a child tracker (Smart Kids) and a smart car tracker to form a Smart Life service.

Figure 5

Consumer and industrial IoT connections in the MENA region



Source: GSMA Intelligence

2.3 Industrial IoT growing the fastest

Adoption of IoT among enterprises will drive overall IoT growth in the region, resulting in industrial IoT connections overtaking consumer in 2018 and forming the majority of connections (57%), reaching 624 million in 2025 (see Figure 5). Governments in the region are both major customers and policy enablers of this industrial IoT.

Utility companies are installing smart meters to monitor customers' use of energy or water in near real-time, cutting costs and helping balance supply and demand. For example, Egypt and UAE utilise IoT-enabled water management to deal with insufficient groundwater reserves. Kuwait's Ministry of Electricity & Water in partnership with Zain and SAP is connecting over 1 million smart electricity and water meters, enabling real-time access to usage and billing data.

The region has shown strong interest in connecting assets within a city and creating smart mobility solutions, with several countries (including Saudi Arabia, Qatar, UAE and Egypt) committing to smart cities as part of Vision 2030. Dubai, for example, is targeting 30% of public transport to be autonomous by 2030.

As traditional sources of income such as oil shrink, UAE, Saudi Arabia and Kuwait are investing in renewable energy and emerging technologies. Some Gulf states have revealed plans to cut emissions, and improve energy efficiency and climate mitigation. For example, in UAE, Tabreed has implemented sensors across the region to improve how the company sends cool air to people.

Smart buildings will continue to be the largest industrial segment throughout the forecast period, followed by smart metering.

The region has been targeting the opportunities enabled by IoT technologies, with examples including the following:

Saudi Arabia: Neom, a new smart city being built on a greenfield site in Saudi Arabia, is receiving $500 billion from the country's public investment fund and local/international investors. Neom allows Saudi Arabia to reinvent the city as eco-friendly and traffic free, where mobility is combined with other initiatives such as remote working policies, holograms and an emphasis on walkability. It will provide residents with future-proof infrastructure, with urban design optimised to provide a choice of transport to make the city more liveable for residents, including the disabled. The kingdom's three-stage plan sees electric vehicles, autonomous trains, robo taxis and trucks in the medium term (5-10 years) and autonomous pods in the long term (10+ years).

Turkey: In its 2013–2023 action plan, the Ministry of Transport & Infrastructure in Turkey has stated its intent for all cities to introduce smart traffic systems that change depending on vehicle speed, as well as digital bus stop and traffic signs. The third most populated city in Turkey, Izmir, has deployed a fully adaptive traffic management system that allows real-time integrated traffic management to improve road safety.

Egypt: An agreement between Honeywell and the state's Administrative Capital for Urban Development has been signed to ensure that the new administrative capital of Egypt has state-of-the-art security infrastructure. The intention is to integrate security and surveillance systems into a unified control point, giving a citywide view to enable more efficient deployment of response units.

In 2018, Huawei launched its second OpenLab in the region, following its Dubai facility which focuses on public safety, smart grid, smart city, smart government and smart education. Cairo's Openlab has four centres – one each for Partner Development, Joint Innovation, Talent Training & Certification and Industry Experience. Huawei aims to develop services and solutions through industry and academic alliances and partnerships at the facility.

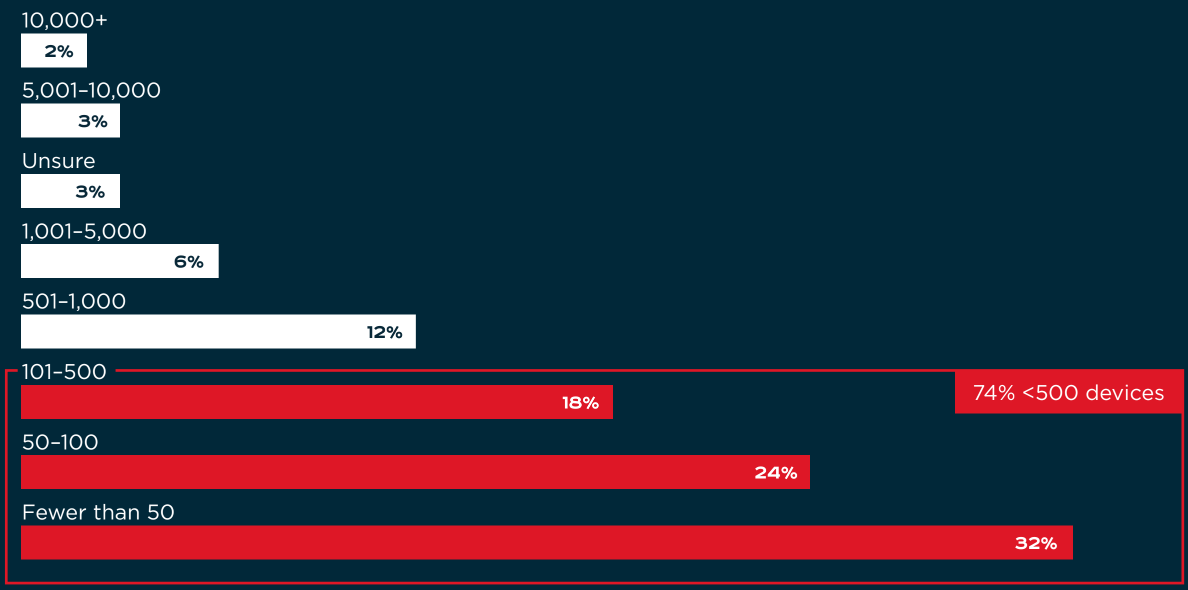
UAE: The Roads and Transport Authority in Dubai has approved a five-phase $161 million smart traffic system project aimed at reducing congestion and improving response time to accidents. In 2017, the Dubai police force welcomed a robotic policeman to their team. If successful, more will be deployed around the city to collect evidence, identify criminals and patrol the streets, with the additional benefit of working 24×7 and reducing the risk of harm to human police officers. Its body contains cameras that use facial recognition. It can also read vehicle number plates and talk to the public.

IoT Enterprise Survey sheds light on IoT deployment

Enterprise appetite for IoT is strong. While larger businesses may be receiving the most attention, most of those deploying at present count as SMEs, including some very small companies.[4] GSMA Intelligence recently surveyed enterprises with upwards of 20 employees; this revealed at a global level that almost two thirds of businesses had deployed an IoT solution by the end of 2018.[5] Turkey has the highest rate of enterprise IoT deployments globally, with 68% of businesses having already deployed. Globally, most deployments are small – 74% of existing deployments count fewer than 500 IoT devices (see Figure 6).

Figure 6

Global IoT deployment size (by number of devices)



Source: GSMA Intelligence

This is also reflected in Turkey, where 80% of enterprises deployed fewer than 500 devices, and 50% fewer than 50 devices. Existing deployments are centred on increasing operational efficiencies and the management of supply chain, assets and fleets. Since IoT requires significant investment, companies are prioritising activities that offer immediate return – though in Turkey enterprises also measure success of deployments in terms of compliance with regulation (37%, compared to a 30% global average). Challenges remain around integration, security and cost, regardless of company size, but in Turkey enterprises highlighted different challenges to those globally; for example, integrating IoT technology with existing technology was a main challenge globally (47%); in Turkey this was at 38%. The country’s number one challenge was a lack of in-house skills (45%). Unclear return on investment (RoI) is also felt more by Turkish enterprises (33%) compared to globally (22%).

[4] Company size definitions: small = 20-99 employees, medium = 100-500 employees, large = 500+ employees

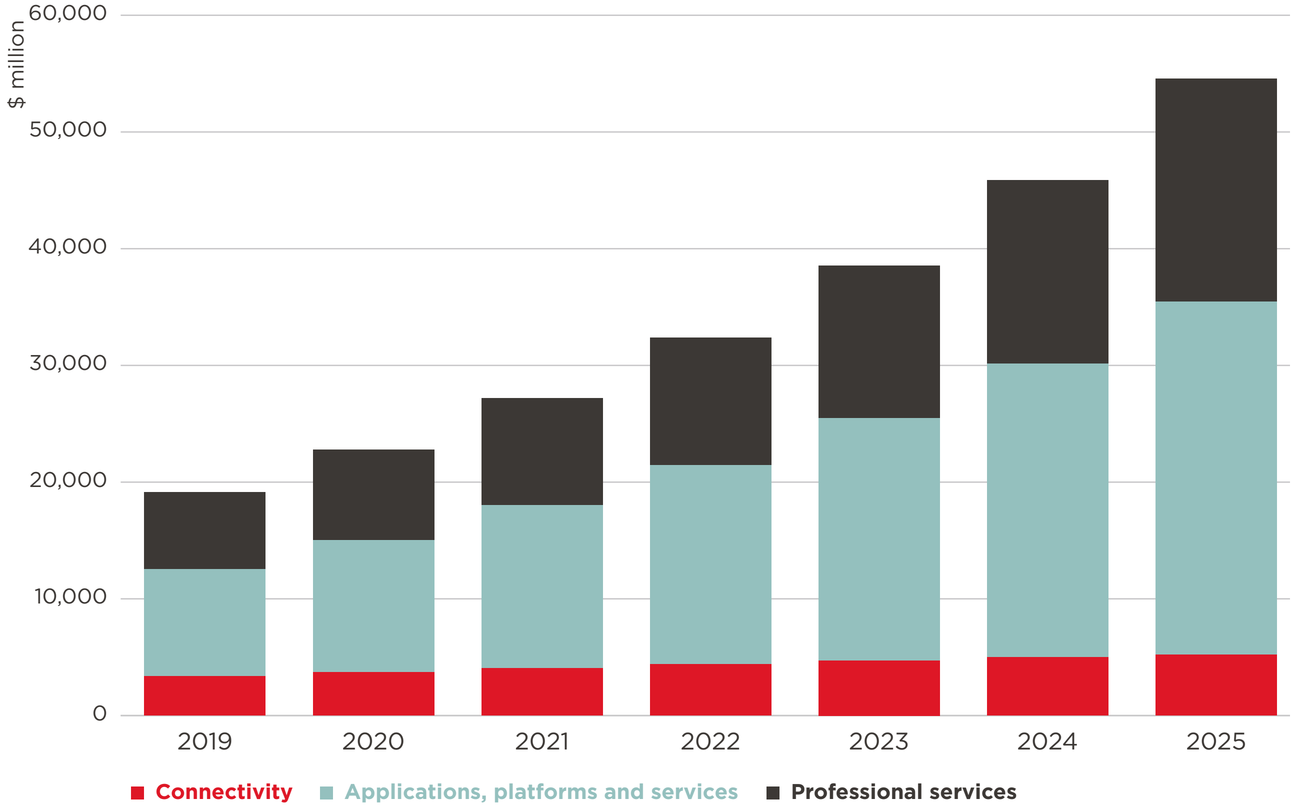
[5] IoT in Business: the enterprise voice on the adoption, GSMA Intelligence, 2018

2.4 The IoT market opportunity in MENA

IoT revenue,[6] for all ecosystem players in MENA, will increase at a CAGR of 19% to 2025 to reach $55 billion (see Figure 7). Applications, platforms and services[7] are expected to increase as a share of IoT revenues over the forecast period, growing from 44% to account for 55% by 2025.

Figure 7

IoT market revenues in MENA



Source: GSMA Intelligence

Players from a range of backgrounds, including telecoms, IT, device manufacturing and systems integration, are all vying to capture a portion of the market opportunity. Although connectivity revenue will grow, representing an opportunity for mobile operators in particular, it will account for just 5% of total IoT revenue by 2025. For this reason, regional operators have been expanding their capabilities beyond connectivity to capture a larger proportion of the overall market value.

However, the IoT ecosystem is complex and fragmented (see Figure 8), and the boundaries between traditional technology, IT and OTT players are blurring as new business models emerge around data, analytics and services. This makes it difficult for any single company to provide end-to-end solutions. Having the right strategic alliances and partnership agreements in place is key to success in IoT, reducing the time to market and streamlining the process for governments and enterprises when it comes to sourcing an IoT solution.

[6] For GSMA Intelligence, IoT revenue excludes device and module chipset revenue but includes revenue associated with provision of connectivity, applications, platforms and services, and professional services

[7] Includes revenue associated with the provision of vertical-specific IoT solutions and services; connectivity and device management platforms; data analytics; cloud storage and security services

Figure 8

IoT ecosystem and example players in MENA

Professional services (consulting, systems integration, managed services)	Revenue associated with strategic and operational planning, use case development and other IoT-related advisory services	Accenture IBM TCS
	Revenue associated with the entire process of the design, build and implementation of an IoT solution	Atos Infosys Tech Mahindra Wipro
	Revenue associated with the contractual outsourced management, usually on a recurring basis, of the different layers within the IoT value chain	Capgemini CGI Cognizant Innova
Security	Revenue associated with the provision of device, network, applications and services security	NTT Data Gemalto Secureworks
Data analytics	Revenue associated with analysing data produced from IoT devices	Amazon Google IBM Oracle
Cloud	Revenue associated with the cost of storing IoT device data in the cloud	Alibaba Cloud AWS Microsoft Azure
Applications	Revenue associated with AEP provision, which accelerates and simplifies the development of applications, providing common, reusable horizontal solution components	Fujitsu General Electric Honeywell Somfy
IoT platforms: application enablement platforms (AEPs); device management platforms (DMPs); connectivity management platforms (CMPs)	Revenue associated with DMP provision, enabling remote management of IoT devices	Cumulocity HPE SAP
	Revenue associated with CMP provision, which facilitates the delivery of data communication service on mobile and other networks, private APN, fixed IP and VPN	Comarch Ericsson Nokia
	Revenue associated with the provision of vertical-specific IoT solution and services	Cisco Jasper Huawei PTC
Connectivity	Connectivity and traffic revenue associated with connecting IoT devices using cellular, LPWA, satellite or fixed networks	Etisalat Vodafone Turkcell LoRa

Source: GSMA Intelligence

The GSMA Intelligence IoT Enterprise Survey showed that operators in Turkey are well placed as IoT solution providers compared to other countries; 14% of enterprises chose operators as their first-choice IoT solution provider compared to 10% globally. Asked what IoT proposition operators should offer, 58% of Turkish enterprises point to being most interested in receiving a bundle of IoT connectivity and IoT devices or modules, compared to 48% globally.

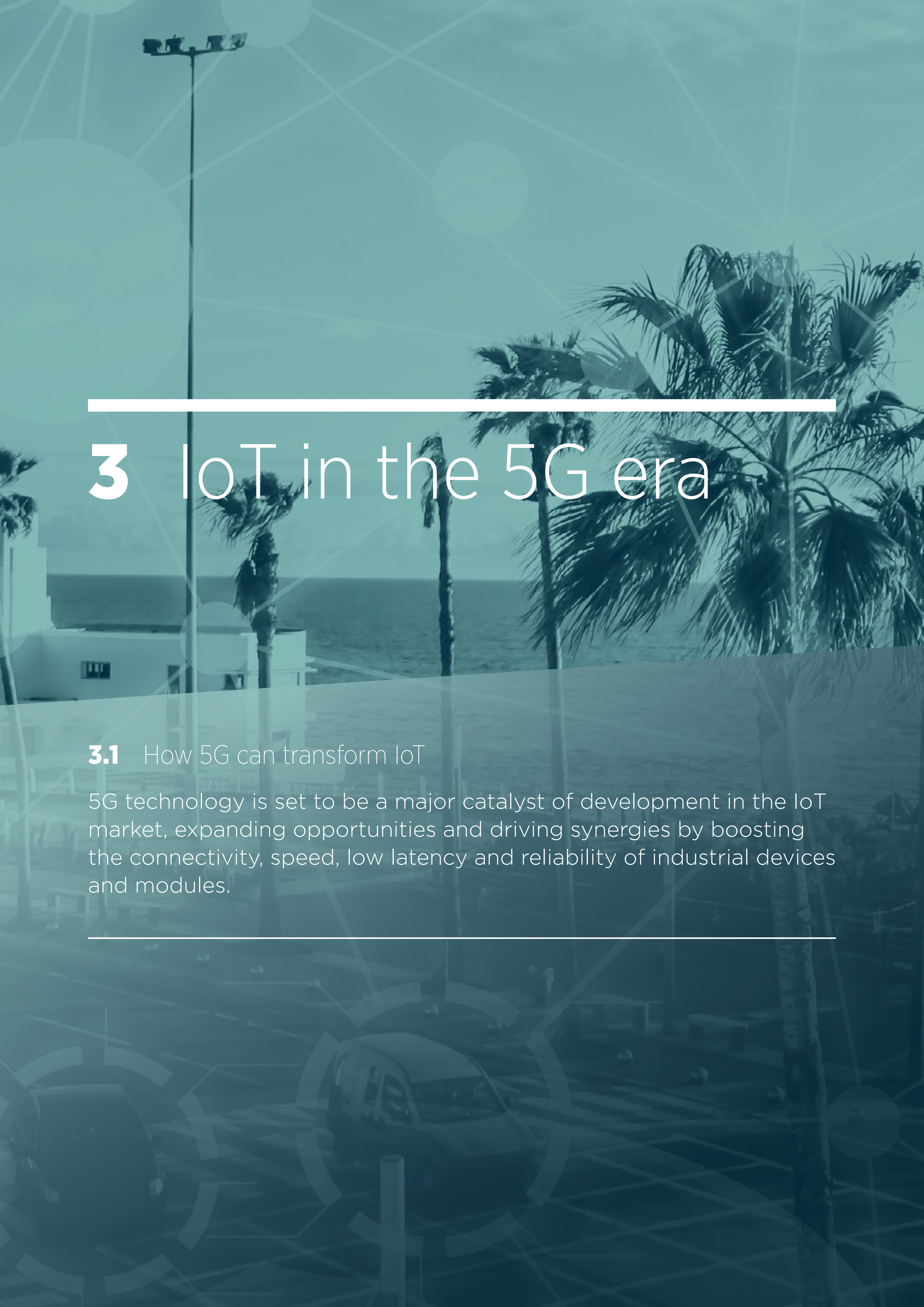
Some operators in the region have moved beyond just providing connectivity. For example, STC Saudi Arabia includes a variety of services in its portfolio such as an end-to-end solution for fleet monitoring, including tracking devices, connectivity, software and support. The operator has invested in IoT platforms, cloud and cyber security, expanding its data centre to handle the additional traffic. Similarly, Vodafone Egypt offers fleet management, smart meters and cloud/hosting solutions to move into applications, platforms and services. Bundling around connectivity enables operators to offer a powerful proposition.

Some operators can take advantage of having in-house IT expertise. For instance, Innova, the systems integrator and solution provider arm of Turk Telekom, has launched the SkywaveIoT Partner Programme. This enables enterprises, start-ups and manufacturers to develop and integrate applications on the platform, giving enterprises access to expertise in product development, marketing and new partnership opportunities.

2.5 Operator-led IoT applications and partnerships

Operators in the MENA region are finding that partnerships are critical to the success of their IoT solutions. Recent partnerships include the following:

- Du and OLEA, a healthcare incubation platform company, showcased a number of smart health devices at GITEX 2018. A connected medical booth called 'The consult station' allows physicians to diagnose patients remotely through a number of medical instruments in the booth such as blood pressure meters, stethoscopes and thermometers.
- Zain Saudi Arabia and Nokia signed two MoUs to bring IoT services and end-to-end solutions to businesses and the public sector in Saudi Arabia, in line with the country's Vision 2030. One MoU will allow Zain KSA to use Nokia's worldwide IoT network grid (WING). The second MoU is for the two companies to partner to create enterprise solutions in different verticals.
- A sales channel partnership allows STC Solutions (STCS) to resell Ericsson services. This includes hardware, software and training across networks, digital and managed services to end users. Ericsson, STCS and STC together developed digital infrastructure to capture value from IoT and new 5G use cases, as part of Saudi Arabia's Vision 2030.
- Ooredoo Qatar has been growing its ecosystem of partners. During MWC19, it announced a partnership with IT service and consulting company Atos to leverage its infrastructure as a service (IaaS), cloud transformation and cybersecurity. The collaboration was furthered in September 2019 when the companies launched cybersecurity solutions to support secure digital transformation of Qatari companies. Oredoo has also launched an IoT platform, IoT Builder, running on AG Cumulocity, to enable the integration of connected devices with applications for enterprises.
- Turkcell offers vehicle tracking for corporate users through Turkcell Kopilot, with the service now extended to individual users through Turkcell's sales and communication network. The Kopilot device is connected to a car's OBD2 (On-Board Diagnostics 2) and includes an embedded IoT SIM card. It has a dedicated application that informs users of travel statistics and can measure driver performance. It provides data to insurance companies in return for discounts on petrol and other third-party loyalty deals.
- Etisalat UAE offers end-to-end solutions for businesses and governments for smart buildings and smart cities, and is partnering with the Ministry of Interior to deliver a smart fire alarm solution, Hassantuk for Homes. The operator supplies, installs and maintains the system, and uses Etisalat's 4G, NB-IoT networks and AI to monitor and report fires.



3 IoT in the 5G era

3.1 How 5G can transform IoT

5G technology is set to be a major catalyst of development in the IoT market, expanding opportunities and driving synergies by boosting the connectivity, speed, low latency and reliability of industrial devices and modules.

Examples of 5G's benefits for IoT use cases include the following:

- Massive machine type communications (mMTC) has been defined by ITU-R as one of three important categories of 5G use cases. 5G is a key technology enabling mMTC to scale IoT connectivity to a massive number of devices with diverse quality-of-service (QoS) requirements.
- 5G will benefit LPWA technologies by enabling transmissions to penetrate walls in urban environments, to travel further and reach more devices.
- Critical services such as autonomous driving, remote surgery and automated manufacturing will benefit from high-speed, ultra-reliable low-latency communication (URLLC) delivering sub-millisecond latency with super low error rates from minimal packet loss.
- 5G expands the use of real-time data to help create cost-effective operational efficiencies and future-proof businesses.
- Network slices enabled by 5G can be used to isolate IoT devices in terms of traffic, control and resources, significantly enhancing security and efficiency to protect critical systems from attack.
- Combining mobile edge computing (MEC) with 5G enables data processing and analytics to take place closer to the IoT device, minimising traffic across the network and reducing latency. The resulting performance enables real-time analytics, improves connectivity and helps minimise data privacy risks.

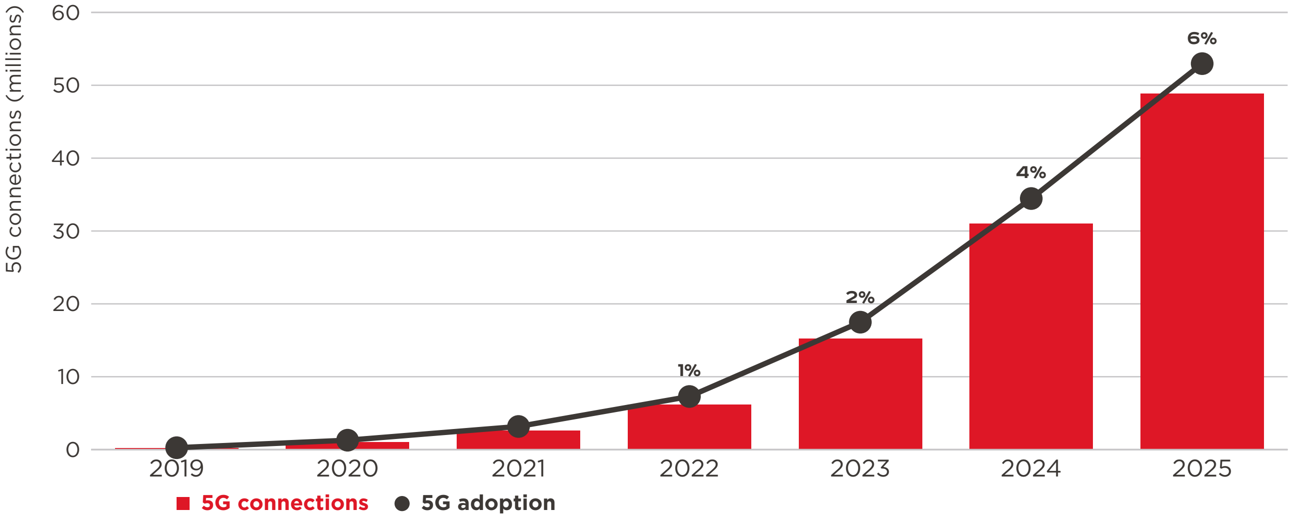
Such benefits from the convergence of 5G and IoT are likely to be mitigated by a considerable increase in the security threat coming from a significant expansion in IoT end points and the softwarisation of the 5G supply chain, particularly in non-standalone deployments where 5G interfaces with 4G networks. Operators worldwide will need to carry the burden of investing in 5G and overcoming the growing security threat that deploying 5G could bring in terms of systems integration, software interfaces, business processes, technical skills and cultural mindset.

3.2 The 5G landscape expands in breadth and depth

By 2020, more than 50 countries will have launched 5G mobile services across North America, Europe, the Middle East and Asia Pacific. In the Gulf Cooperation Council (GCC) Arab States, 5G is rapidly moving from trials to early commercialisation. By September 2019, nine operators in the region had launched 5G networks: Batelco and Viva (Bahrain), du and Etisalat (UAE), Ooredoo, Viva and Zain (Kuwait), STC (Saudi Arabia) and Vodafone (Qatar), accounting for 25% of global 5G launches at that time. These early 5G deployments are driving a forecast of nearly 50 million 5G connections by 2025 (Figure 9).

Figure 9

5G adoption in MENA
excluding licensed cellular IoT and fixed wireless



Source: GSMA Intelligence

Non-standalone (NSA) deployments will mean 4G and 5G networks coexist and remain complementary for many years, with a densified network of small cells and use of mid-band (1-6 GHz range) and upper-band (above 6 GHz) spectrum to facilitate high-speed data. However, standalone (SA) networks – which involve the use of a 5G core and new radio – will be introduced by some MENA operators in key cities and locations of 5G demand, to leverage the full capabilities of low-latency features. Enhanced mobile broadband will be the key use case in early 5G deployments in the region, enabling developments in applications and content for immersive reality, eSports and enhanced in-venue digital entertainment (stadia, music venues). While fixed wireless is not new in certain MENA markets, 5G could drive momentum as a fixed broadband access solution in rural areas and in countries with limited fibre-to-the-home (FTTH) penetration.

3.3 Opportunities for 5G-enabled IoT

In the enterprise space, there is already broad agreement among MENA operators on the key industries where 5G-powered IoT can deliver the greatest long-term value, including manufacturing, smart cities, automotive, logistics and utilities. Industrial IoT in particular could offer the strongest opportunities for 5G-enabled IoT solutions in the MENA region. Companies embarking on their own Industry 4.0 transformation will be using autonomous robots, big data analytics, AI, virtual reality and drones among others to implement smart data-driven manufacturing. They will be looking for enhanced product quality, predictive maintenance to reduce machine downtime, and the ability to monitor processes through the entire product lifecycle. Successful implementation of these new technologies and the resulting efficiencies will require companies to integrate the enabling technologies of IoT and 5G together. Potential synergies from the combination of 5G and Mobile IoT overcome the existing limitations of use cases, to the benefit of all.

Take for instance unmanned aerial vehicles (UAVs), or drones: existing connectivity for these typically relies on point-to-point satellite control, which requires large numbers of control stations along the flight path. The need to build and maintain such stations increases costs and limits the range at which most drones can operate, making them unviable for deployments in many remote locations in MENA. The combination of LTE and 5G changes this, allowing the range and flexibility of non-line-of-sight transmission, while enabling cutting-edge security through the on-board SIM.

Another example of the synergistic pairing of IoT and 5G technologies is highly relevant in the Gulf states. The region is still heavily reliant on oil and gas assets. Across the 20+ countries in MENA, between 20% and 40% of GDP[8] is based on oil and gas or oil-reliant government activities such as construction that are heavily dependent on oil-funded government contracts. The security vulnerabilities of the oil and gas industry have recently been brought sharply into focus at the same time as 5G IoT solutions are emerging. The performance and security of the oil industry, so critical to the region, can be significantly enhanced through the effective deployment of 5G-enabled IoT solutions. EY analysis (the Future of IoT)[9] points to opportunities in the oil industry, including centralised surveillance monitoring, production process analytics, refinery equipment maintenance, and – critically in today's difficult international environment – digital security operations centres (SOCs) for protecting operational technology. The ability of national operators in the region to support the protection and management of oil and gas assets will not have gone unnoticed by national governments and operators.

[8] The political economy of MENA oil exporters in times of global decarbonisation, Tagliapietra, 2017

[9] Future of IoT, EY, 2019

4 Policy enablers for sustainable IoT development

Regulators in MENA are in the unique position of being able to design IoT policy enablers at a pace close to that of the market's development. In the US and Europe regulations are playing catch up with IoT suppliers that already have products and solutions on the market, and with businesses already implementing IoT solutions. For example, it was only in 2018 that various government bodies in the US called for guidelines and regulations on IoT devices. In the UK, meanwhile, the National Cyber Security Centre introduced guidelines on best practices for consumer IoT devices in 2018. However, mobile operators in the US and Europe launched M2M and then IoT products in the late 2000s.

The consequence of this long gap between deployment and regulation is the risk that insecure IoT devices in the field become too expensive or difficult to protect against cyber-attacks. Companies that offer IoT products and services are equally as responsible for IoT security as businesses that utilise the resulting IoT data. As shown in Figure 10, vulnerable IoT deployments can become easy targets for malicious actors to cause disruption, whether simple inconveniences or those with life-or-death consequences.

Figure 10

Most common types of cyber-attack

Distributed denial of service (DDoS)

- IoT devices weaponised as malware-infected machines to repeatedly direct traffic to overwhelm a server, network or website.

Objective: to cause an unexpected shutdown of operations.

Malware

- Malicious software, in the form of viruses, worms, spyware or ransomware.

Objective: to enable attackers to install more malware, spy on data and information, cause system breakdowns and hold data for ransom.

Ransomware

- A type of malware that blocks access to systems and crucial information, withholding these for ransom.

Objective: to disrupt normal operations and raise illegal funds.

Man-in-the-middle attacks (MITM)

- Digital eavesdropping where attackers intercept the flow of data.
- Usually occurs on insecure connections e.g. public Wi-Fi.

Objective: to filter and steal data.

Advanced persistent threats (APT)

- A catch-all term for concerted attempts to establish a long-term malicious presence in a network.
- The term reflects the attacker’s resources and technical skills, as well as the intensity of such attacks.

Objective: to mine sensitive data.

Source: GSMA intelligence

4.1 Security by design in IoT deployments

IoT companies are positioning their offerings to business to achieve two goals: to help them improve productivity and efficiency, and to grow revenue with existing and new customers. When they make decisions on whether to include security as part of their IoT products, they compare the expected cost and future benefits.

Regulatory requirements can influence a change in behaviour and empower authorities to enforce it. The European Union's General Data Protection Regulation (GDPR) is wide-ranging in scope and reach, aiming to shift the security conversation from cost burden to business enabler. GDPR sets a maximum financial penalty of either 4% of global revenue or €20 million, whichever is higher. In the cost/benefit analysis, fines will refocus investment to arrive at an optimal security solution. For example, it is impractical in effort and financial terms for any business to aim for the most secure IoT solution. A truly secure "end-to-end" IoT solution requires security elements at each layer to be a continuous and dynamic process throughout the solution's lifecycle. Diversity in IoT means this theoretical goal is also uneconomical to fit every type of device, module and solution. From the beginning, GDPR forces IoT companies and businesses to align their security aspirations with the known financial penalty and expected impact on the wider IoT value chain.

Outside of regulations, guidelines are also helpful in encouraging the adoption of security by design. The UK issued a voluntary code of practice to embed security-by-design principles in consumer IoT devices in October 2018. International standards organisation ETSI also introduced a global standard for consumer IoT devices such as connected toys, connected household gadgets and smart home assistants. The GSMA issued IoT Security Guidelines and Assessments in 2018 to provide practical steps for mobile operators and device manufacturers to protect their IoT products and solutions. Many global operators including Etisalat and Turkcell have leveraged these guidelines to obtain buy-in throughout their organisations to re-consider their security strategies.

4.2 The role of privacy regulations to foster digital trust in IoT

While some countries' laws are more stringent than others, generally, data protection laws set out rules that seek to protect privacy by placing restrictions on organisations regarding how they can collect and use personal data. In an IoT context, individuals risk privacy breaches, for example, through unauthorised spying via insecure IoT devices such as connected surveillance cameras. There is still an insufficient number of businesses building their operations based on privacy-respecting principles, such as the published GSMA Mobile Privacy Principles.

Given that the GDPR is a horizontal law, it covers all organisations processing personal data, including those in the IoT space. However there is no specific IoT privacy regulation in the EU. While the FTC brought a lawsuit against Vizio, a TV manufacturer in the US, for misleading consumers. As opposed to sectoral regulation or enforcement, the implementation of general data privacy laws applies to the processing of all personal data, regardless of the technology used or the sector in which the processing takes place. This helps consumers understand their privacy rights across the digital economy. Fostering digital trust requires an understanding from both consumers and IoT solution providers as to their rights and responsibilities with regard to privacy. Training, standards and regulation are also required for IoT companies and businesses that may not have full knowledge of how to protect individual privacy in IoT deployments.

4.3 Nurturing positive regulation for IoT in MENA

Over the last two years, regulators in a handful of countries in the region have started to consider regulatory frameworks for IoT. The following countries are at various stages with IoT-specific policies:

- **UAE:** in March 2019, the IoT Policy became official following its introduction by the UAE Telecoms Regulatory Authority (TRA) in 2018. As well as the standard requirements that all IoT service providers must be registered, TRA required that the privacy principles as regulated by GDPR be followed in UAE.
- **Saudi Arabia:** in February 2019, Saudi Arabia began an industry consultation for an IoT-specific regulatory framework. It requires that all service providers ensure data management includes security and privacy considerations. As well as these early efforts in IoT, there are several industry-specific regulations and guidelines. For example, the central bank, the Saudi Arabia Monetary Authority, published a Cybersecurity Framework in 2017, to protect critical financial system infrastructure. In 2017, the Saudi National Cybersecurity Authority was established to provide organisational guidelines on cyber defence and governance for companies.
- **Jordan and Oman:** in 2017, the telecoms regulatory bodies in Jordan and Oman started their own regulatory explorations on likely regulations. Jordan explicitly states that security and privacy are similar but also distinct concepts in terms of IoT regulation.
- **Turkey:** the country does not have a specific IoT policy that defines behaviours for data protection. However, its Data Protection Law was introduced in 2016 and closely follows EU GDPR principles.

The common thread running through these regulations is strong security hygiene practices applied across IoT companies and businesses. This helps consumers understand their privacy rights across the digital economy. Some security recommendations are easy tasks; from making sure devices do not have default passwords to requiring basic encryption of devices. As the regulatory landscape in MENA matures, additional themes such as encouraging IoT companies and businesses to conduct a cost/benefit analysis on the optimal security solution will be essential.

4.4 Best practices from the global regulatory environment

The experience of the US and Europe reveals that IoT vendors in highly competitive environments could consider going to market without enough consideration of security, resulting in potentially messy retrofitting and patching when security flaws appear. However, in MENA, regulators have the opportunity to design IoT regulation including security at the early stages of the market, with the potential to develop policy at a similar pace to that of IoT market development.

The following three lessons from US and Europe, related to the rules under which IoT vendors and businesses operate, are applicable to regulators in MENA:

- **Create legislative certainty:** Whatever the precise remedies made available under the law, the objective of a smart data privacy law should always be to encourage good practice in the first place and, in case of infringement, to provide genuine and proportionate redress for individuals who have suffered a significant level of harm. This avoids individuals having to resort to private rights of action and protects organisations from frivolous claims. Without the idea of proportionality or a threshold of significant harm, supervisory authorities may waste resources, and individuals will not be effectively protected. However, regulators should remain aware of the commercial frictions resulting from new policies and the impact this may have on the cost of IoT security.
- **Incentivise multi-layered IoT security:** IoT solutions and applications comprise several components, making the security of IoT not a static exercise but a dynamic and fragmented one. Regulation will need to focus on the security of the ecosystem as a whole, not just individual components. Any regulation that can incentivise IoT vendors and businesses to work together for the greater good of ecosystem security should bring positive results.
- **Develop ongoing security efforts:** an IoT regulatory framework provides the certainty that IoT companies and businesses prefer, but a box-ticking exercise can also drive behaviour to the lowest common denominator for security. There is a role for regulators to gather like-minded businesses keen to build on basic security-hygiene best practices to foster trust. Consideration of data and privacy levers that provide sufficient room to promote innovation through new business models enabled by IoT and 5G can also go a long way.

Industry-led IoT security guidelines and best practices from the GSMA or ETSI provide a much-needed initial step for key stakeholders in the value chain. Furthermore, regulations such as GDPR and the upcoming California Bill SB 327 provide certainty in the cost-benefit analysis for any businesses considering their IoT security strategies. In the MENA region, there is a role for regulators to legislate for a baseline security position with the relevant financial penalties. Businesses in MENA are thus aware of what the bare minimal expectation on IoT security is and can decide how far they wish to position themselves along the security best-practice spectrum.

5 Mobile operators in MENA: a pathway to success in IoT

Operators are foundational to the growth and innovation of IoT in the region

MENA has had good reason to move early and strongly in adopting IoT: to support its leading position on smart cities; to leverage the industrial efficiencies of automation; and to drive growth in its economy. However, sustaining IoT's positive impact on the region will increasingly be driven by mobile operators.

Whether it be the foundational need for 5G network performance to underpin an explosion of IoT services, or the control and connectivity of NB-IoT and the SIM, mobile operators are vital to the IoT market in the region and a leading driver of value-added IoT services.

Building value-added services beyond connectivity is the key to monetisation

Launching LPWA networks, using NB-IoT and LTE-M technologies, has been vital in helping operators in the region to deliver seamless IoT connectivity. However, to create added value solutions and sustainable revenue growth, IoT operators must move beyond connectivity by building on their reputation as trusted industry partners. Operator IoT solutions can deliver substantial benefits to customers such as increased productivity, reduced costs and automated business processes, as well as driving innovative new products and new business models.

Governments play a vital role as both policymakers and customers

IoT deployments requiring critical network performance will rely on 5G capabilities for latency and speed. It is imperative that regulators across the region release sufficient quantities of new harmonised mobile spectrum in all frequency ranges (sub-1 GHz, 1-6 GHz and above 6 GHz) including the mmWave frequencies. Short-term regulatory approaches that seek to maximise licence revenues rather than the wider and more sustainable economic benefits afforded by 5G and IoT synergies could result in slower IoT and dependent economic growth. Governments are customers as well as policymakers, and mobile operators should continue to work closely with national and regional agencies to ensure the regulated reliability and cross-border experience of the mobile industry is a natural choice for governments across the region.

MENA has a strategic opportunity to lead on security by design

In the race to 5G deployment there is a risk that security by design in 5G and IoT networks gets left behind. However, in MENA, policymakers and operators have a strategic opportunity to ensure cybersecurity and data protection is built in from the start. The GSMA and the mobile industry have contributed to the security initiative by introducing the GSMA's IoT Security Guidelines and the IoT Security Self-Assessment. More information on the guidelines and their 85 detailed recommendations can be found at www.gsma.com.

Further reading

IoT: the $1 trillion revenue opportunity, GSMA Intelligence, 2018

The Mobile Economy Middle East & North Africa 2019, GSMA, 2019

5G in MENA, GSMA Intelligence, 2018

5G Landscape Q2 2019, GSMA Intelligence, 2019 gsma.com

GSMA Head Office
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601