OECD*publishing*

IOT MEASUREMENT AND APPLICATIONS

OECD DIGITAL ECONOMY PAPERS

October 2018 **No. 271**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report was prepared by the Working Party on Communication Infrastructure and Services Policy (WPCISP) and the Working Party on Measurement of the Digital Economy (MADE). The report reviews different definitions of the Internet of Things (IoT) in view of an operational definition with corresponding subcategories for the CDEP work, and explores feasible ways to measure IoT and its implications for infrastructure and networks. It concludes by proposing a framework (i.e. taxonomy) of IoT for measurement purposes.

This paper was approved and declassified by written procedure by the Committee on Digital Economy Policy on 27 September 2018 and was prepared for publication by the OECD Secretariat.

This report was drafted by Alexia Gonzalez Fanfalone with contributions received by Pierre Montagnier and Sam Paltridge from the OECD Secretariat.

This publication is a contribution to the OECD Going Digital project, which aims to provide policymakers with the tools they need to help their economies and societies prosper in an increasingly digital and data-driven world.

For more information, visit www.oecd.org/going-digital.

#GoingDigital

Note to Delegations:
This document is also available on O.N.E. under the reference code:

DSTI/CDEP/CISP-MADE(2017)1/FINAL

Table of contents

Tables

Figures

EXECUTIVE SUMMARY

The Cancun Ministerial mandate on the Digital Economy highlighted the importance of developing IoT metrics to assess the effects of the IoT in different policy areas (OECD, 2016[1]). Accordingly, this report reviews different definitions of IoT in view of establishing an operational definition for the CDEP work, and proposes a taxonomy for IoT measurement. The report also explores potential challenges for communication infrastructures due to the exponential growth of IoT devices through the application of connected and automated vehicles. This IoT application was chosen as the data transmission requirements of fully automated vehicles may have substantial implications for network infrastructure, and therefore may require prioritisation in terms of measurement.

The report endorses the existing OECD working definition of IoT with the exclusion of devices that are already taken into account in OECD metrics (i.e. smartphones, tablets and PCs), and proposes to add subcategories for measurement purposes. The OECD overarching IoT definition would be, "*The Internet of Things includes all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals. While connected objects may require the involvement of devices considered part of the "traditional Internet", this definition excludes laptops, tablets and smartphones already accounted for in current OECD broadband metrics."*

To better inform policy making, this report proposes a framework (taxonomy) with a breakdown of IoT into categories given that many connected devices will have different network requirements. For example, critical IoT applications such as remote surgery and automated vehicles will require high reliability and low latency connectivity, whereas Massive and disperse Machine-to-Machine (M2M) sensors used for agricultural applications may not be that sensitive to latency or network speeds.

Within the IoT proposed measurement framework, the two main categories of IoT proposed are: Wide Area IoT, and Short Range IoT. The Wide Area IoT category includes devices connected through cellular technology as well as those connected through Low Power Wide Area Networks, whereas the Short Range IoT category includes devices using unlicensed spectrum with a typical range up to 100 metres. Within the category of Wide Area IoT, two subcategories are further suggested: 1) Massive M2M devices (e.g. sensors for agriculture or smart cities), and 2) Critical IoT applications (e.g. remote surgery applications, fully automated vehicles and other industrial robotics applications).

IoT Measurement and Applications

1. Introduction

The term Internet of Things (IoT) refers to the connection of an increasing number of devices and objects over time to the Internet. As highlighted in the Cancun Ministerial, following the convergence between fixed and mobile networks, and between telecommunication and broadcasting, the IoT represents the next step in convergence between ICTs and economies and societies on an unprecedented scale. It holds the promise to substantially contribute to further innovation, growth and social prosperity, and as with any such development, policy makers and other stakeholders need evidence to inform the decisions they will take in the coming years. As such, the Cancun Declaration invited the OECD to further develop work on these emerging technologies, including the Internet of Things, in order to fully embrace their benefits, and to strengthen the collection of internationally comparable statistics.

The IoT is expected to grow exponentially, connecting many billions of devices in a relatively short time (OECD, 2015[2]). Some of these connected devices will be in private residences, related to function such as energy management, security or entertainment. Others will be associated with developments in areas such as transport, health and manufacturing. A key question, therefore, is how to prioritise measurement efforts of those elements of the IoT that are of most relevance to policy makers. For example, in the case of IoT use in manufacturing, sometimes called Industry 4.0 or the next production revolution, decision makers will likely wish to know not only how many robots are in operation in their country but also how many are connected. At the same time, they will not only need to know how many automobiles and trucks are connected but, in the case of fully automated vehicles, what are their potential demands on communication infrastructures in terms of generating large amounts of data.

Developments around connectivity or the implications of new demands placed on networks are not, of course, new to stakeholders in communication markets. The pervasiveness of such developments does, however, raise questions about the best ways to collect the information that ultimately proves necessary to inform policy. For instance, what is the best source to collect data on connected robots? The producers of robots or the suppliers of the connectivity? Similarly, what is the best channel to gather information on autonomous vehicles? The vehicles' registries that exist in all countries or the producers of those vehicles or those providing connectivity?

There will be issues as well that are a high priority for communication policy and regulation especially, where the demands of the IoT develop in ways that have strong implications for the location, deployment and capabilities of infrastructures. As a single fully automated vehicle, for example, may generate far more data than several thousand mobile wireless users, this may have profound implications for decisions in areas such as spectrum, rights of way, the location of data centres, requirements for faster broadband access, and backhaul to name just a few. At the same time, others will look for information that informs considerations in areas such as privacy and security, as well as interoperability, numbering and standardisation. Therefore, statistical definitions and indicators of IoT should reflect, as much as possible, the different policy interests and objectives around this area.

Apart from being better informed on future demand for communication infrastructures, including those where public investment may be involved, there is a second critical reason measurement in this area, which is important for policy makers. It is the ability to measure the effects of the IoT on productivity, GDP and growth, as part of the Digital Economy. However, to assess any measure of the influence of IoT on GDP, the first step is to have a proper indicator of the size of the IoT. This latter point was made clear in a recent publication (2018) by the Bureau of Economic Analysis in the United States (BEA), which endeavoured to measure the influence of the digital economy on GDP. Although the BEA recognised the IoT[1] as an important element of the digital economy, it was excluded given the inherent measurement difficulties, as well as the complexity to allocate the "digital" component of the connected devices when accounting for the value added (Barefoot et al., 2018[3]).[2]

The Cancun Ministerial Mandate identified a set of areas for stakeholder engagement to promote IoT deployment. In particular, it highlighted the importance of developing metrics to measure the effects of adoption of the IoT in different policy areas (OECD, 2016[1]). In this respect, the aim of this report is twofold. First, to review different definitions of IoT in view of an operational definition for the CDEP work. Second, to explore feasible ways to measure IoT and its implications, notably for infrastructure and networks. The potential challenges for infrastructure will be discussed in a case study: the developments of connected and automated vehicles.

The structure of this report is the following. Section 2 provides a short overview of the main IoT measurement questions that have arisen in the past few years among OECD countries. Section 3 summarises the IoT definition used by the OECD to date and how the OECD has measured Machine-to-Machine (M2M) communications since 2012. Section 4 provides an overview of the selected definitions and measurement efforts by diverse government authorities, organisations, as well as market players. Section 5 addresses the question of whether certain categories of IoT devices require prioritising in terms of measurement given their potential implications for communication infrastructure (e.g. automated vehicles). Section 6 provides a short overview of emerging regulatory and policy challenges related to the IoT that underline the importance of measurement. Finally, Section 7 concludes by highlighting some criteria to take into account in terms of IoT measurement, and proposing a working definition of IoT for OECD countries, with its corresponding subcategories.

2. Measurement questions/issues

To date, the OECD has gathered data on the number of machine-to-machine (M2M) connections on cellular wireless networks. Many of these M2M connections have been used for legacy applications built directly on mobile networks. However, as IoT devices increasingly become Internet Protocol (IP) based and platform-agnostic (i.e. operating on mobile, fixed, and other networks), how should OECD countries seek to measure the number of such devices and their implications for telecommunication networks?

Most residential IoT devices are not directly connected to a telecommunication operator network; rather, they connect either through a "smart-home hub" or through residential wireless networks. There are, however, significant differences between these devices, both in terms of numbers of devices and network uses, and the Internet-enabled devices, which have proliferated in private residences in recent years, which tend to be user-focused (personal computers, tablets, smartphones, wearable devices and so forth).

At the same time, many applications of IoT such as for public utilities or government use private networks, and thus might not appear in supply-side data (i.e. telecommunication operator provided). Reporting data in an area such as connections for smart metres, for example, is likely to be provided by the associated service providers even if telecommunication networks furnish the underlying connectivity. On the other hand, there will likely still be a need for some data to be provided by network operators as a separate category.

Different IoT applications (i.e. massive and disperse M2M communications versus critical IoT applications) are likely to have diverse network requirements. For instance, Ericsson has said that automated vehicles will require low latency (i.e. lower than 5ms) and 100% network reliability and coverage. At the same time they say massive dispersed connected M2M objects, such as sensors, will require 100% network coverage, a 10-year battery life but are not really sensitive to latency (Ericsson, 2017[4]).[3] This highlights the need to prioritise measurement according to policy goals.

While IoT data use has been relatively modest to date, a question can be raised as to how are next-generation applications, such as fully automated vehicles, industrial IoT devices and so forth, are expected to change the data use profile of these devices in the future? As an example, according to some estimates, a single autonomous vehicle will produce 4 000 GB of data per day, --i.e. the equivalent of data produced by 3 000 smartphones, (Intel, 2016[5])--, or even 100 GB of data per second (CNBC Autos, 2017[6]). According to other estimates, a connected car generates 20 GB of data per day (Seminconductor Engineering, 2017[7]).

A question is then, how will a substantial increase in data affect infrastructure requirements? Which amount of the collected data will be actually transferred and how much more network capacity will be needed? At the same time, are their categories of devices that use SIM cards that deserved being broken out in the data collected by authorities given the different demands they make on infrastructures? In other words, information about automated vehicles may be more critical than objects such as luggage, environmental sensors or the many thousands of different types of things that may one day be connected via SIM cards (simply because they generate less traffic).

2.1. Specific questions that arise with regards to presently used M2M metrics

As new technologies start to emerge, such as the eSIM (embedded SIM) in wearable devices a question can be raised as to how to take into account these new SIM cards in M2M measurement. The Apple Watch Series 3, for example, uses and eSIM while many Android Wear 2.0 watches have to date used a standalone "Nano SIM". Should such devices be considered as a single or multiple connections? In other words if one of these devices is connected to an existing smartphone service account and the other potentially transferable over different accounts should they be counted differently?

If such devices are recorded as multiple connections, should they be counted under traditional mobile broadband connections (e.g. smartphones, tablets) or under connected devices such as automobiles and sensors are today? In terms of the element related to single or multiple connections, it is understood telecommunication providers count a single vehicle as a single connection even if it has two SIM cards perhaps provides a way forward.

Will special types of enhanced connected devices that currently use M2M SIM cards, such as automated vehicles, require a separate category in order to track high data consumption of these devices (as opposed for example to data consumption from connected devices relying only on sensors) in order to adapt network architecture and communications infrastructure accordingly?

In addition, a further question that could be asked for device manufacturers and mobile operators, is: when a device, such as a smartphone, has multi-homing of connectivity (e.g. it is able to use LTE-M and LoRa networks), is there a double accounting of M2M devices that use SIM cards and are LPWA connected devices?

A comprehensive list of questions and issues in terms of IoT measurement, and in particular concerning current M2M measurement, can be found in Annex A.

3. What is IoT?

3.1. OECD current working definition of IoT and M2M

The OECD defines IoT in broad terms “including all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals. This includes laptops, routers, servers, tablets and smartphones, often considered part of the “traditional Internet”. However, these devices are integral to operating, reading and analysing the state of IoT devices and frequently constitute the “heart and brains” of the system. As such, it would not be correct to exclude them” (OECD, 2015[2]).

In addition to IoT, Machine to Machine (M2M) communications, as a subset of IoT, is characterised by autonomous data communication with little or no human interaction (OECD, 2015[2]). In fact, the OECD 2012 report on the subject defined M2M as, “Devices that are actively communicating using wired and wireless networks that are not computers in the traditional sense and are using the Internet in some form or another. M2M communication is only one element of smart meters, cities and lighting. It is when it is combined with the logic of cloud services, remote operation and interaction that these types of applications become “smart”. RFID can be another element of a smarter environment that can be used in conjunction with M2M communication and cloud services” (OECD, 2012[8]).

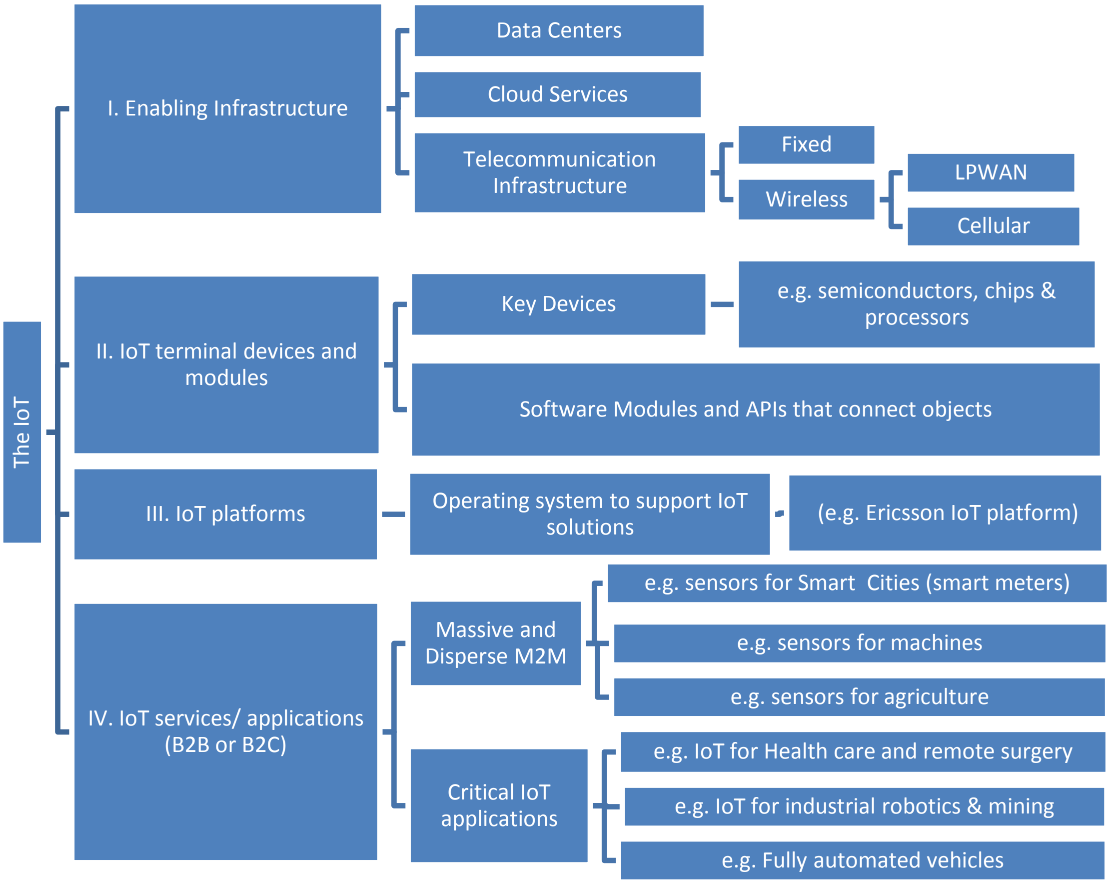
In terms of the OECD’s IoT definition it has mainly been used to date to inform policy and regulatory discussion rather than to define the IoT for data collection. It is, therefore, broad for practical reasons. On the other hand, the authorities that collect these data (e.g. telecommunication regulators) as well as the GSMA have defined M2M.

The first challenges in arriving at a definition of IoT for measurement are to consider questions such as what may be practical, what may be the priorities and so forth. Such a concept may, for example, take into account key enablers (i.e. M2M communications, big data, cloud computing and sensors) leading to machine-learning applications (OECD, 2015[2]). Furthermore, measuring the amount of “connected devices” when multiple devices are connected in an integrated system can prove challenging. The following underlying technologies are key enablers that are required for IoT devices to function properly:

- semi-conductors (i.e. sensors, chips, processors, memory, and so forth)
- modules and devices (i.e. software/API connecting the IoT devices)
- IoT platforms (i.e. the operating systems and support existent IoT solutions)
- the network (i.e. connectivity where standardisation and interoperability issues are relevant).

The different components of the IoT enabling environment can be illustrated in a diagram (Figure 1).

Figure 1. IoT enabling environment



Note: This diagram was conceived taking into account the IoT frameworks in Japan, France, and Korea.
Source: Own elaboration.

In each key-enabling layer of the IoT, numerous economic actors are involved. This can have an influence on defining IoT for measurement purposes, and eventually on how the data may be collected. For example, some of the players involved are the following:

- the designers and producers of connected devices sold to consumers (e.g. a Samsung connected television or Amazon’s virtual assistant, Alexa)
- the IoT module providers (i.e. chips, processors, software and APIs)
- network equipment providers (e.g. Ericsson, Cisco, Huawei)
- IoT cloud providers (e.g. Amazon, Google)
- IoT platform providers (i.e. the integral support software that connects everything in an IoT system facilitating communication, data flow, and device management)
- connectivity providers (e.g. LoRa, SigFox, mobile operators, fixed and satellite providers).

Future work on measurement of IoT could focus on mapping the different actors from a supply side perspective for data collection purposes. This mapping could include stakeholders who define connectivity protocols, those who build their own IoT LPWAN network and make it available to customers, those who act as intermediaries by connectivity based on third party networks, and so forth.

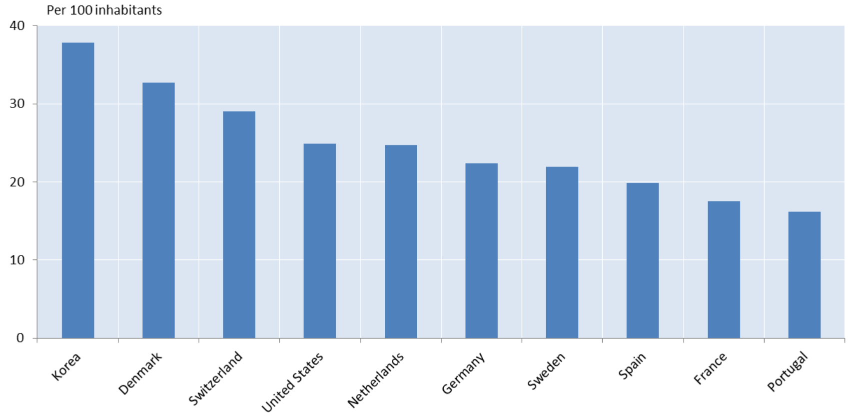
Given that the IoT is part of an ecosystem with key enablers, it has proven challenging to find a sufficiently precise definition for measurement purposes. Nevertheless, many of the existing definitions used for IoT, are well suited to support general concepts for policy discussions (see Annex B for selected examples).[4] In some cases, some intergovernmental bodies have addressed regulatory issues surrounding IoT without defining it. For instance, the Body of European Regulators for Electronic Communications (BEREC) has worked in recent years on studying the impact of IoT on regulation and how to foster an enabling environment for IoT without committing to a definition (BEREC, 2016[9]).[5]

There are ongoing efforts by intergovernmental organisations and international standardisation bodies to harmonise a definition of the IoT for measurement purposes. One example is that as part of BEREC's Programme of Work and Budget for 2018. BEREC plans to assess what type of measurement of IoT European National Regulatory Authorities (NRAs) are already conducting on the supply-side and/or on the demand-side, and to assess if there is, at this stage, any common set of IoT-related indicators which BEREC could regularly collect in the future (possibly from 2019 onwards).[6] Another notable example is the International Organisation for Standardisation (ISO) who is currently working on the definition and vocabulary of the IoT, as well as the interoperability of IoT systems (platforms) as part of their technological standards projects (ISO, 2018[10]).

Previous work from the OECD has highlighted the difficulty to measure IoT (OECD, 2017[11]; OECD, 2015[2]; OECD, 2016[1]). It has been underlined that, "*Measurement of the number of IoT devices connected to the Internet has proven hard to obtain, with countries only now starting to collect data.*" In the absence of official statistics, one option has been to examine private sources of data collection.

One source, among others (e.g. CISCO, Ericsson, and so forth), which has been used in previous OECD publications, is data provided by Shodan, which describes itself as a search engine for Internet-connected devices. In 2015, according to Shodan's definition there were 363 million visible devices online with some 84 million recorded in the People's Republic of China (hereafter "China") and 78 million to the United States (Figure 2). While recognising that such data collection is nascent and there is no consensus to date on definitions, such approaches provide one option for the future.

Figure 2. Devices online per 100 inhabitants, top OECD countries



Note: Last updated: 29-May-2015.
Source: OECD Digital Economy Outlook 2015, http://dx.doi.org/10.1787/888933473770 using data from Shodan.

One approach to the measurement of IoT is to focus on a subset or subcategory. The OECD has collected data from communication authorities on M2M embedded SIMs since 2012. Likewise, the GSMA collects M2M data from its membership. While a very important part of the IoT, this category is only a small part of all devices that are now connected or will be so in the future.

3.1.1. OECD measurement of M2M data

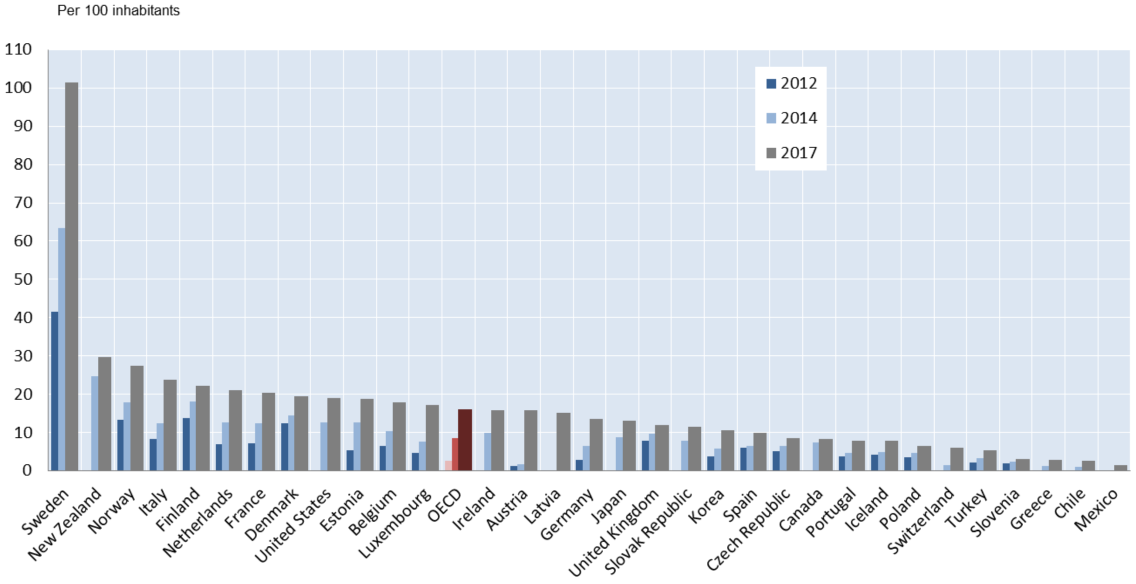
The Broadband Portal publishes information on key telecommunication market indicators from communication regulators and official statistical agencies in the OECD area. Within the set of indicators, most OECD countries now collect data on M2M SIM cards.

To calculate the number of M2M/embedded mobile cellular subscriptions, the OECD defines M2M on mobile networks as "*the number of SIM-cards that are assigned for use in machines and devices (cars, smart meters, and consumer electronics) and are not part of a consumer subscription*". This means that dongles for mobile data and tablet subscriptions should be counted by countries under the mobile broadband definition, whereas SIM-cards in personal navigation devices, smart meters, trains, automobile etc., should be counted under the M2M category.

One can observe an increasing trend in M2M SIM card subscriptions in the OECD area when comparing the latest data (June 2017), with M2M penetration data for the years 2012 and 2014 (Figure 3).

Figure 3. M2M/embedded mobile cellular subscriptions per 100 inhabitants

Years 2012, 2014 and 2017

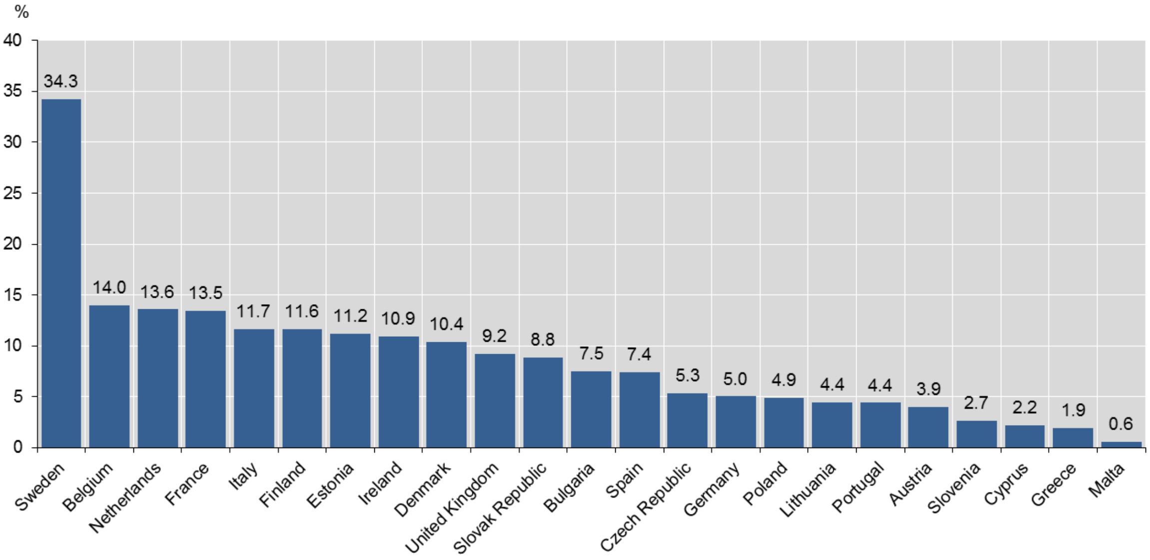


Note: For Korea, provided data does not include some devices (personal navigation devices etc.) as they are based on different technologies rather than SIM cards.
Source: OECD, Broadband Portal, www.oecd.org/sti/broadband/oecdbroadbandportal.htm.

The M2M data shows only where the SIM cards stem from (i.e. where the numbers are assigned or from which national MNO or MVNO the SIM is allocated to the end-user), but not where the connected device is used. Therefore, it may be the case that a country displaying high rate of connected M2M SIM cards reflects the fact that a domestic MNO or MVNO player is strong in the international IoT-M2M market (e.g. Telenor in Sweden). For example, Telenor Connexion, which held 81% of the Swedish M2M market (December 2016), uses its numbering (IMSI numbers) for not only Sweden, but also their clients around the world.[7]

One factor that will likely increase these M2M penetration figures is the trend by National Regulatory Authorities (NRAs) in several countries to allow the use of extra-territorial M2M numbers (e.g. Germany, Netherlands and Belgium). Historically, MNOs have used their IMSI numbering in the country that supplied the numbers. In recent years, however, regulators in countries such as Belgium and the Netherlands have moved to more open policies around use of numbering and M2M. In this sense, it is notable that both these countries have large shares of the EU M2M market, substantial above the equivalent shares in other countries in the European Union, and placed second and third behind Sweden (Figure 4).

Figure 4. Share of M2M SIM cards* over total SIMs in EU countries, October 2016**



Note: *Definition by EC of M2M SIMs: "M2M is about enabling the flow of data between machines and machines and ultimately machines and people. Regardless of the type of machine or data, information usually flows in the same general way -- from a machine over a network, and then through a gateway to a system where it can be reviewed and acted on." – www.m2mcomm.com.

**Note by Turkey: The information in this document with reference to "Cyprus" relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Turkey recognises the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Turkey shall preserve its position concerning the "Cyprus issue".

Note by all the European Union Member States of the OECD and the European Union: The Republic of Cyprus is recognised by all members of the United Nations with the exception of Turkey. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

Source: Data from European Commission Digital Single Market, EU 28, "Financial indicators, fixed and mobile telephony, broadcasting and bundled services indicators – 2016" (European Commission, 2017[12]), https://ec.europa.eu/digital-single-market/en/connectivity

3.2. Aspects to consider when defining and measuring IoT

Some of the first questions to consider in relation to a definition of the IoT are whether it is practical for the purpose of measurement and the elements it should include. Such a concept could take into account key enablers (i.e. M2M communications, big data, cloud computing and sensors) leading to machine-learning applications (OECD, 2015[2]). That being said, when multiple devices are in a system, measuring the amount of "connected devices" can be complex. The following list is not exhaustive, but highlights some key aspects to be considered in relation to the measurement of the IoT:

I. Measuring "connected devices" by features (allowing, among other things, to distinguish M2M data traffic versus mobile communications traffic). These characteristics include:
    a. Dispersion or concentration of devices/applications;
    b. Mobility (stationary or nomadic objects),
    c. Data volume and network performance (bandwidth), and
    d. QoS including security standards and sensitivity to latency.

II. Categorising IoT by technological options for their use and adoption:
    a. Sensors and simple hubs (i.e. sensors gather and analyse environment information, and hubs connect these sensors to a broader network such as air-conditioning, electricity, security systems);
    b. Integrating hubs (i.e. a system that connects simple hubs creating more complex devices such as Apple's HomeKit that bundles electric power, home security, window shades into one system);
    c. Enhanced applications (i.e. services that collect and analyse data from connected devices and the environment in real time such as "automated vehicles").

III. Taking into account the underlying IoT infrastructure that enables communication among devices (i.e. cloud services, quantum and edge computing, data storage, mobile networks, LPWA networks, backhaul and backbone connectivity and so forth).

The current OECD definition of the IoT provides a conceptual framework to guide policy discussions, as it encompasses the universe of connected IoT devices (i.e. the definition mentions "*all devices or objects whose state can be altered via the Internet, with or without the active involvement of individuals*"). It could, however, be rendered more useful by adding subcategories for measurement purposes. These subcategories could be based on different features of the devices: i) range of IoT devices (i.e. wide-area or short range), or ii) the type of M2M connection (i.e. simple sensors, or critical "live" IoT devices such as automated vehicles). The benefits of complementing the OECD definition by adding subcategories could be manifold. Namely, two main benefits are mentioned here. One, it would render the issue of measuring the IoT more tractable, and two, it would allow for prioritisation in data collection in certain categories (or subcategories) of IoT that may have more influence in communication infrastructure.

In the future different IoT-M2M applications are likely to generate very different usage patterns. Environmental sensors, for example, may only generate very small amounts of data relative to connected bicycles and robots, right up to perhaps the largest amounts in the case of automated vehicles. Thus, a breakdown of IoT into several subcategories such as "Massive Machine to Machine communications" (e.g. sensor like M2M), and critical IoT applications (e.g. automated vehicles) seems an advisable way forward in order to better inform policy makers.

In summary, concerning IoT metrics, there is a question of definition, and a question of measurement. The subsequent section provides an overview of the definitions by several stakeholders (including the private sector), as well as describing how they have used these definitions to measure the IoT.

4. Other IoT Definitions and current estimates of the size of IoT

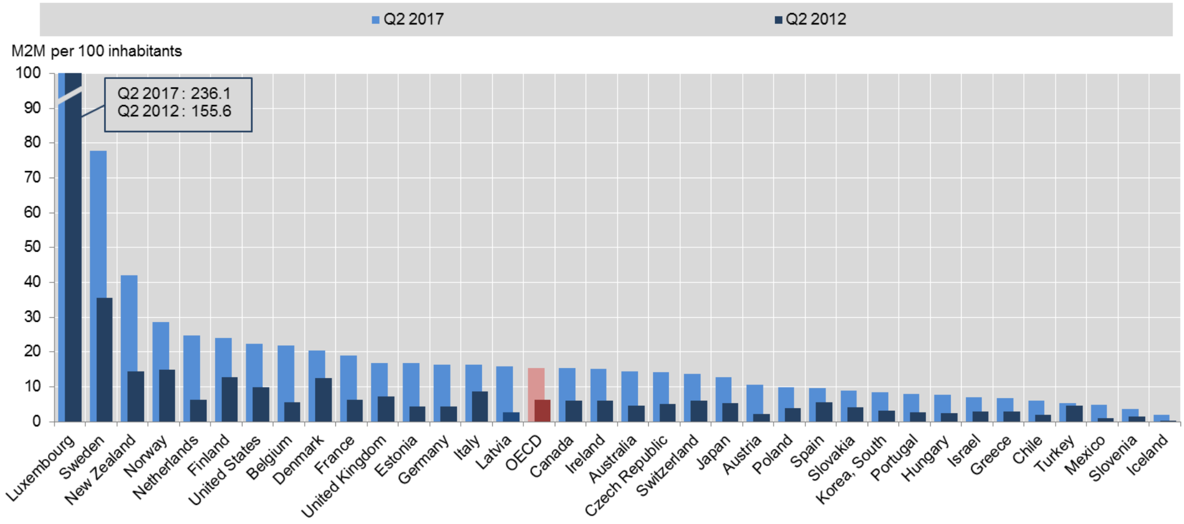
4.1. GSMA

The GSMA states that although IoT is a very complex and diverse ecosystem with very limited reported data, they define it as, “IP enabled devices capable of two-way data transmission (excluding one-way communication sensors and RFID tags). Includes all access technologies e.g. cellular, short-range, fixed and satellite.”

The GSMA also has a working definition of M2M cellular connection, which they use to track the number of M2M connected objects over the years by country. Their M2M definition is “A unique SIM card registered on the mobile network at the end of the period, enabling mobile data transmission between two or more machines. It excludes computing devices in consumer electronics such as e-readers, smartphones, dongles and tablets.” This means that certain applications that are regarded as IoT/M2M according to other definitions are not counted in the GSMA data.[8] According to GSMA data on M2M penetration, the number of M2M SIM cards in every OECD country has increased from 2012-2017 (Figure 5).

Figure 5. M2M connections per 100 inhabitants, GSMA data* for OECD Countries**

Type the subtitle here. If you do not need a subtitle, please delete this line.



Note: *Population data from OECDstat and M2M data from GSMA Intelligence. **Luxembourg is not shown in the graph. According to the communications regulator, the Institut Luxembourgeois de Régulation, there were 89 400 M2M SIM cards at the end of 2016, whereas GSMA reports 1 377 000 M2M SIM in Q2 2017.
Source: Own elaboration using data from GSMA Intelligence database.

4.2. The private sector

McKinsey (2015) defines the IoT as, “sensors and actuators connected by networks to computing systems. These systems can monitor or manage the health and actions of connected objects and machines. Connected sensors can also monitor the natural world, people, and animals." Their definition excludes, "systems in which all of the sensors' primary purpose is to receive intentional human input, such as smartphone apps where data input comes primarily through a touchscreen, or other networked computer software where the sensors consist of the standard keyboard and mouse" (McKinsey Global Institute, 2015[13]). The McKinsey Global Institute used this definition in a report that endeavoured to estimate the total potential economic effects of IoT across nine different settings (e.g. vehicles, homes, cities, factories, logistics, health, and so forth). According to this report, the potential effects ranged from USD 3 trillion-11.1 trillion per year in 2025 (McKinsey Global Institute, 2015[13]).[9]

Ericsson measured 16 billion connected devices in 2016, out of which 5.6 billion corresponded to IoT. They estimate that by 2022 there will be 29 billion connected devices, out of which 18 billion will be IoT related (Barboutov et al., 2017[14]). A relevant feature regarding the IoT definition by Ericsson is that PCs, laptops, tablets, mobile phones and fixed phones are excluded. As noted previously with the GSMA M2M definition, this means that certain applications that are regarded as IoT/M2M are not counted in the Ericsson data. In addition, Ericsson breaks down IoT into two subcategories: wide-area and short-range IoT. The short-range segment mostly refers to devices connected by unlicensed spectrum (e.g. devices using Wi-Fi, Bluetooth and Zigbee with a typical range up to 100 metres). This category also includes devices connected over fixed-line Local Area Networks (or LANs) and powerline technologies.[10] The wide-area segment consists of devices using cellular connections (e.g. NB-IoT and Cat M1 technologies), as well as unlicensed low-power technologies such as Sigfox, LoRa and RPMA.[11]

As defined by Ericsson, currently, the most common technology in the wide-area IoT segment is GSM/GPRS, and according to them, the Compound Annual Growth Rate (CAGR) between 2016 and 2022 for wide-are IoT and short-range IoT is expected to be 30% and 20%, respectively (Barboutov et al., 2017[14]). It is notable that the 2017 Mobility Report by Ericsson has a change in the definition of these two segments with respect to their 2016 report, which only referred to cellular and non-cellular IoT.[12]

Furthermore, given the data requirements of different IoT applications, Ericsson points out that within the wide-area IoT segment, two distinct sub-segments have emerged: massive and critical applications. On the one hand, massive IoT connections require high connection volumes (but small data traffic), are usually low cost, and require low energy consumption (e.g. smart buildings, transport logistics, fleet management, smart meters and agriculture sensors). On the other hand, critical IoT connections require ultra-reliability and availability of the network, low latency connectivity and high data throughput (e.g. traffic safety, automated cars, industrial applications, remote manufacturing and healthcare, including remote surgery).

The Ericsson Mobility Report further notes that the first cellular IoT network supporting massive IoT applications deployed using LTE networks (based on LTE-Cat-M1 or LTE-M and Narrow Band-IoT technologies), were launched in early 2017 (Barboutov et al., 2017[14]).

CISCO publishes regularly the Virtual Network Index (VNI) Global Mobile Data Forecast, which projects mobile traffic by types of data. CISCO treats as synonymous the definition of M2M and IoT. They define M2M as technologies that "allow systems to communicate with other devices of the same capability, such as utility metering, security and surveillance, fleet management, GPS and navigation, asset tracking, and healthcare record devices" (CISCO, 2017[15]).

In the most recent publication of the CISCO VNI they have made a methodological change. In the February 2016 update, within the M2M category, they have updated the forecast to include low-power wide area network (LPWAN) connections "which is an emerging ultra-narrowband M2M connectivity alternative for a variety of IoT applications". CISCO's M2M definition includes wearable devices, which are "devices capable of connecting to and communicating with the network, either directly through embedded cellular connectivity or through another device (primarily a smartphone) over Wi-Fi, Bluetooth, and so forth" (CISCO, 2017).

According to CISCO's definition of IoT, in 2016 there were 780 million M2M connections around the world, out of which 325 million were wearable devices (e.g. smart watches, smart glasses, health and fitness trackers, wearable navigation devices, smart clothing, and so forth.). Of these wearable devices, 11 million already had embedded cellular connections (i.e. eSIM) in 2016. Their forecast is that by 2021 there will be 3.3 billion M2M connected devices, i.e. a fourfold growth in five years. In addition, the share of M2M connections as part of the total mobile connections is likely to grow.

According to CISCO VNI data, in 2016 M2M devices represented 9.7% of global connected mobile devices (a total 8 billion mobile-connected devices, including M2M modules in 2016), and this share will grow up to 28.4% in 2021 (out of the 11.6 billion forecasted mobile connections in 2021). One factor influencing the growing adoption of IoT to is the emergence of wearable devices (CISCO, 2017[15]).

Some mobile operators now report the amount of IoT devices connected to their networks in their annual financial statements to shareholders. In the United States, AT&T was one of the first companies to report the number of connected devices, and by 2017 had 39 million (AT&T, 2017[16]). More recently, other large players have joined in reporting such data such as operators in China. In 2017, China Telecom and China Mobile, reported 44.3 and 229 IoT devices, respectively (China Telecom, 2017[17]; China Mobile, 2017[18]).

4.3. Telecommunication Authorities in OECD countries

4.3.1. ANACOM the communication services regulator in Portugal

ANACOM has been collecting M2M data since 2012 (e.g. number of M2M devices with SIM cards, traffic and revenues), in the same manner as many other regulators in the OECD area. In 2016, for the first time, ANACOM tried to collect data on Low-Power Wide Area (LPWA) communications technologies (e.g. revenues, number of devices, clients and traffic). The response rate of this survey was quite low; however, based on the very limited number of replies, they found that: 1) there are a small number of (corporate) clients, 2) a large number of devices, and 3) very low levels of traffic on LPWA networks.

On the issue of definition and measurement of the IoT, ANACOM's point of view is that a harmonised methodology is preferable. Concerning metrics, besides usage (revenues, data, devices, clients), ANACOM considers that coverage of IoT should also be studied. In this respect, ANACOM notes that BEREC is developing a report on 5G coverage obligations ("Best practices report on coverage obligations with a view to 5G").

In their view, the GSMA approach is an example of how it is possible to collect data on M2M on a harmonised way across several geographies using supply side data. It could make sense to split these indicators by technology/standard in order to gain some insights on the types of applications that are being offered (i.e. critical or non-critical IoT connections).

However, mobile operators' data will only cover the wide area segment applications of IoT based on licensed spectrum. Concerning applications based on unlicensed spectrum, the suggestion from ANACOM is to contact directly the LPWA providers (e.g. Sigfox, LoRa) which are mostly transnational companies, in order to gather information on LPWA communication.

As for the low range IoT segment, industrial applications and home applications will probably involve different metrics and data sources. From ANACOM's previous experience, possible sources of data for residential services and devices are not directly connected to a telecommunication operator's network. These sources include:

- Retail outlets' and device vendors' retail figures: For several years, ANACOM has collected data from these sources with regards to digital TV devices (through a third party) with good response rates and covering most of the Portuguese market.
- Household surveys: ANACOM has been surveying usage of OTT services for several years based on household surveys.

In addition, ANACOM, the Portuguese communications regulator, highlights the need to refine M2M indicators. Many IoT applications, they note, will be based on cellular networks, and thus, it is possible to rely on traditional data sources (i.e. mobile operators) to collect data on the number of connections, traffic, and even revenue associated with M2M. For ANACOM, it would make sense to further refine M2M indicators in the following ways:

- Collecting data by network/technology (e.g. 2G, 3G, 4G, and 5G).
- Collecting data by subcategories of different network/technologies associated with different M2M and IoT applications (e.g. wide area/short range, critical/non-critical);
- Collecting M2M statistics for specific applications (e.g. automated vehicles).

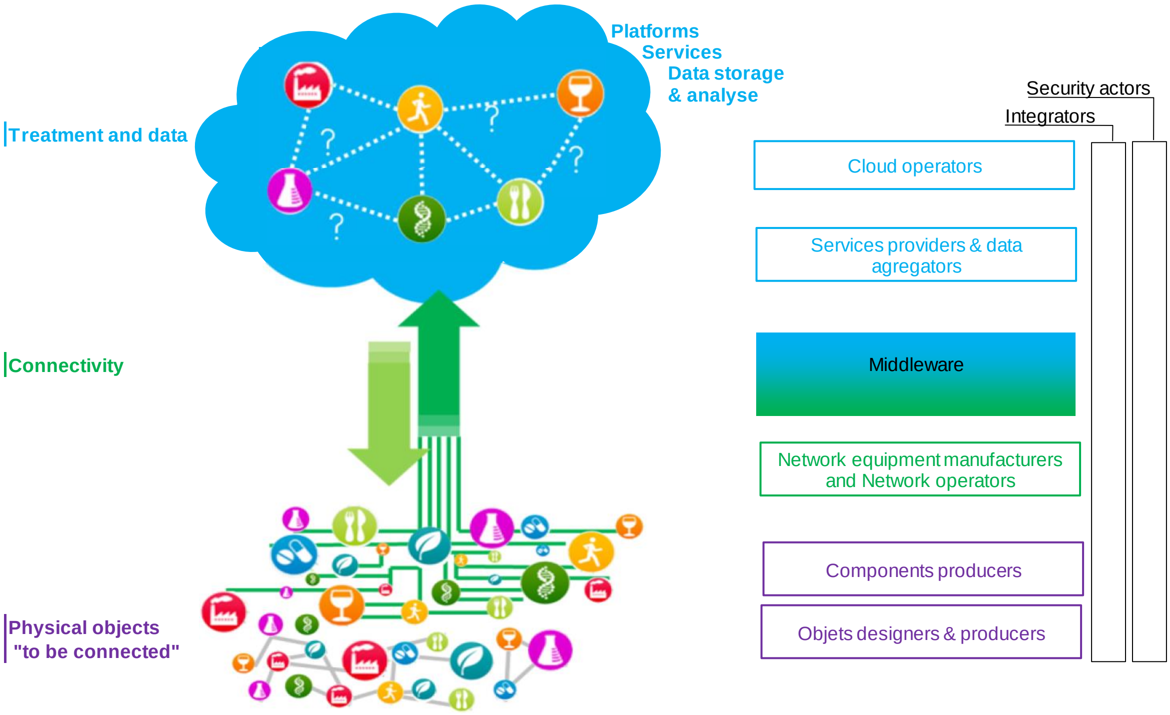
Likewise, in their view, an identical approach can be followed for LPWA services. A related issue concerns mobile penetration measurement. ANACOM says M2M connected devices should be excluded not least because they otherwise render measures of penetration less useful.

Finally, ANACOM expresses that it would make sense to measure adoption of IoT related technologies and applications among enterprises, especially in the case of short range applications and private networks for which alternative data sources may not be available. An example of this is Eurostat's ICT usage enterprise survey, which included a module on the use of cloud services.

4.3.2. ARCEP, the communication services regulator in France

According ARCEP, various components should be considered in the IoT ecosystem. These include the physical objects themselves, the economic actors, the connectivity (i.e. "backbone" of the IoT), and the data flows among connected objects (Figure 6).

Figure 6. ARCEP's components to be considered in the IoT ecosystem



Source: « Le Livre Blanc : Préparer la révolution de l'Internet des objets », (ARCEP, 2016[19]).

As such, ARCEP views the IoT as an ecosystem, and since 2016 has published several reports on the IoT (ARCEP, 2016[19]). In their view, the physical objects to be connected to the Internet can be designed for a large variety of applications, ranging from "smart devices" (i.e. home equipment) to simple elementary components. The economic actors producing those objects similarly range from object designers and producers to network equipment manufacturers. The network layer is crucial, they say, as it ensures the quality of the connexion needed to transmit the data among objects. In this regard, ARCEP notes that in addition to existing traditional communication networks, new dedicated networks are emerging (e.g. Low Power Wide Area Network (LPWAN) providers such as Sigfox, LoRa, and so forth.).

From the perspective of IoT market players and sectors, ARCEP has pointed out several markets where already concrete IoT applications are expanding. For example, some applications include: *i)* "smart territories", which relates -within the communities development projects- to the communicating infrastructures (transport, energy, water) and the optimisation of their management; *ii)* connected buildings (home and work); *iii)* Industry 4.0; *iv)* automated and connected vehicles; *v)* digital health; and *vi)* agricultural enterprises (ARCEP, 2016[19]).

4.3.3. BNetzA the communication services regulator in Germany

BNetzA has defined M2M for the first time in the numbering plan concerning IMSIs (BNetzA, 2016[20]). It defined M2M as "*the predominantly automated exchange of information between technical devices such as machines, vending machines, vehicles or measuring equipment (e.g. electricity, gas and water meters) or between the devices and a central data processing unit. Communications can be either wire-based or wireless. A* *human is not usually involved in the communications, although limited human involvement does not preclude classification as M2M communications. If limited human involvement is part of a service, this does not preclude classification as M2M communications for the purposes of the numbering plan at least in the following cases:*

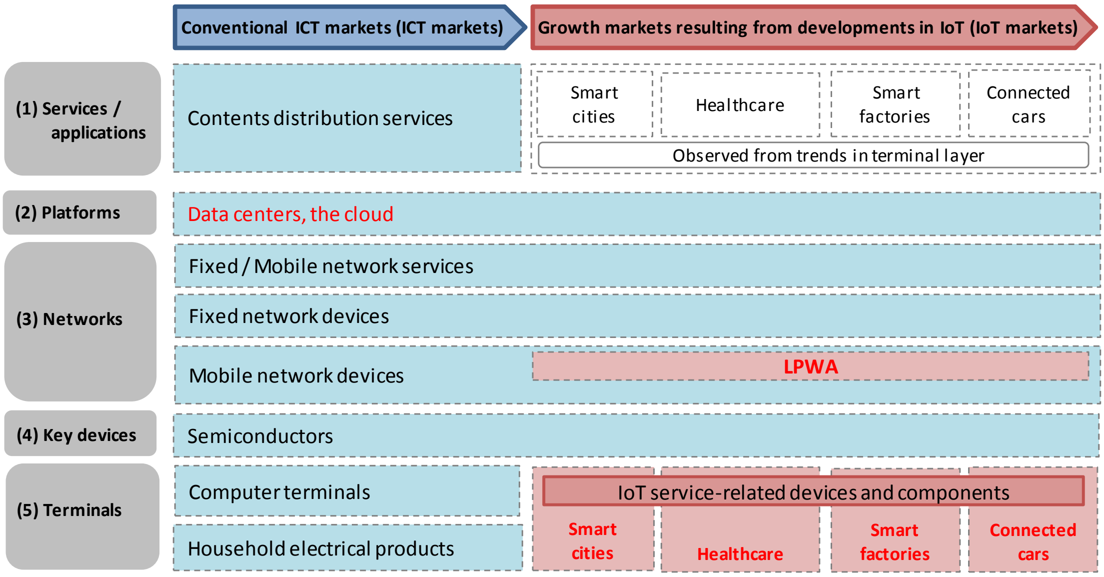
- *activation/operation/control/monitoring of an M2M application or an M2M device using technical equipment such as a computer, smartphone, tablet, etc. by a human in either a private (e.g. smart home) or an industrial environment;*
- *Activation of an application that enables individual communication in the sense of a preselected point-to-point communication but not a call to a freely selectable number. Examples of this are eCalls in vehicles, private emergency calls in lifts and/or vehicles, and concierge services in vehicles.*

This list is not exhaustive and is without prejudice to an assessment of new business models" (BNetzA, 2016[20]). A similar definition is used in the Numbering Plan for Mobile Numbers (BNetzA, 2017[21]). According to BnetzA, in Germany the amount of M2M SIM cards has increased from 1.6 million in 2010 (BNetzA, 2011[22]) up to 7.7 million at the end of 2016 (BnetzA, 2017[23]).

4.3.1. MIC, the Ministry of Internal Affairs and Communications in Japan

The MIC follows a framework when analysing the development of the IoT, which is comprised of several layers (Figure 7).

Figure 7. Market categorisation framework of IoT and data distribution in Japan



Source: "*2017 White Paper, Information and Communication in Japan*," (MIC, 2017[24]).

Japan positions IoT devices according to the wireless communication system supporting it, within a double dimension of distance and power consumption.[13] Taking a similar approach, a report by McKinsey in 2017 provided a multidimensional matrix connection between IoT connectivity solutions (broken down by detailed technology segments and possible IoT related devices), distance, power consumption, bandwidth, and thirteen broad economic sectors (McKinsey, 2017[25]).

The framework developed in Japan also includes a market categorisation characterised by an anticipated growth in the IoT. Four main markets are identified for the future development of the IoT: smart cities, healthcare, smart factories and connected cars. The selected market segments highlighted by Japan significantly overlap with those pointed out in the ARCEP IoT framework (ARCEP, 2016[19]).

4.3.2. OFCOM the communication services regulator in the United Kingdom

The 2017 Ofcom Communications Market Report defines an M2M connection as “a connection between devices, often wireless, where human input is not necessarily required. Commonly used examples of M2M are in smart metering (where the meter reports energy use back to a central billing database) and burglar alarms, which may contain a SIM card to enable communication with monitoring offices. Vending machines are another common example, as some use M2M to keep a central computer up to date with stock levels.” (Ofcom, 2017[26]) It is notable that the active mobile subscriptions measured by Ofcom include M2M connections. However, even if their definition encompasses a broader scope of IoT, Ofcom only measures M2M cellular subscriptions, i.e. a subset of IoT and M2M, and do not keep track of NB-IoT or LTE-M connections.

According to this measure by Ofcom, in the United Kingdom, M2M subscribers have increased from 4.1 million in 2011 to 7.6 million in 2016 (Table 1).

Table 1. United Kingdom telecommunication market: key statistics (selected indicators*)

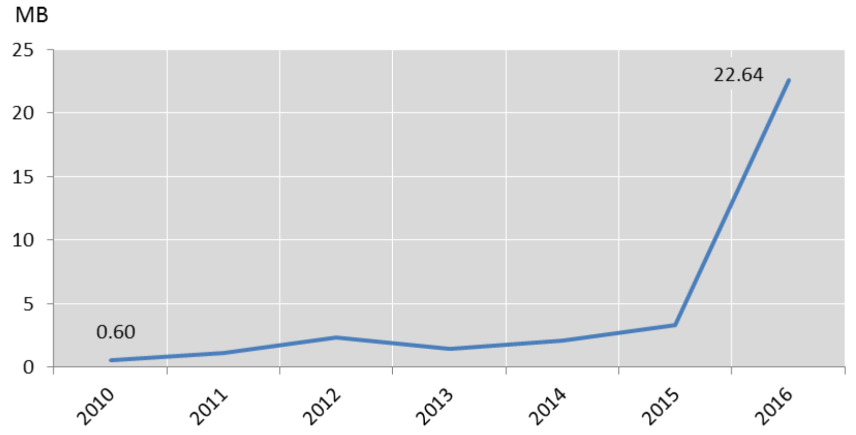
Year	2011	2012	2013	2014	2015	2016
Average monthly mobile data per active connection (GB)**	0.1	0.2	0.4	0.5	0.9	1.3
Active mobile subscribers (millions)***	86.5	88.4	88.8	90.3	91.9	92
4G subscribers (millions)			2.7	23.6	39.4	52.4
M2M subscribers (millions)	4.1	5	5.7	6.3	6.7	7.6

Note: * Selected indicators from Figure 4.1 of the Communications Market Report 2017 (Ofcom, 2017[26]); **average monthly mobile data per active connection for 2011 as of March 2012-16 as of June of each year; ***active mobile subscribers include machine-to-machine subscriptions.
Source: Ofcom / operators / Ofcom Connected Nations Reports 2011–16 (Ofcom, 2017[26]).

4.3.3. PTS, the communication services regulator in Sweden

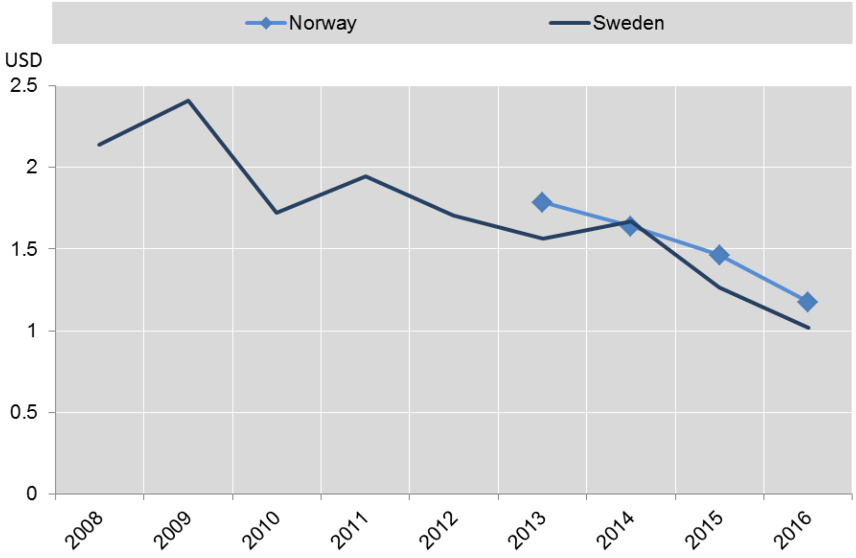
Sweden has some of the most advanced M2M data collection by gathering information on how much revenue is generated per year by M2M subscriptions. Furthermore, since 2010, PTS has collected data on the amount of M2M traffic. While still relatively small when measured per M2M subscription, compared to smartphones, such traffic grew from less than 1 MB per M2M subscription in 2010 to 23 MB in 2016 (Figure 8). Notable, however, was the sharp increase in 2016. There are two potential explanations for this trend. The first one relates to measurement error, as PTS reports that the data provided from Telia up until 2015 had been incorrect, which means that data volumes up until 2015 may be higher than Figure 8 indicates. The second reason for the increase may be the evolution in the M2M market with some application of the technology being used in areas that generate higher amounts of traffic such as connected automobiles.

Figure 8. Monthly M2M data traffic per subscription (MB) in Sweden



Note: PTS defines Machine-to-machine as communication between machines used for telematics and telemetry. PTS defines subscriptions as contract subscriptions plus pre-paid cards. Pre-paid cards are reported according to the 3-month rule. The increase in traffic for data services between 2015 and 2016 depends on Telia's reporting. Telia reported for 2016 around 2 000 Tbyte and for 2015 76 Tbyte. Telia says that the 2015 data is too low but an actual value is not available.
Source: The Swedish Post and Telecom Authority, May 22, 2017.

Figure 9. Monthly revenues per M2M subscription (USD) in Sweden and Norway



Note: Machine-to-machine is communication between machines used for telematics and telemetry. For Sweden, “Subscriptions” is equal to contract subscriptions + pre-paid cards. Pre-paid cards are reported according to the 3-month rule. The M2M subscriptions of both countries was taken from "Telecommunication Markets in the Nordic and Baltic Countries", June 2017, Table 1, http://statistik.pts.se/en/nordic-baltic-telecom-market/tables/mobile-call-and-data-services/table-1-subscriptions/.
Source: Own calculation using data from the Swedish Post and Telecom Authority, May 22, 2017, and the Norway National Communications Authority, https://ekomstatistikken.nkom.no/#/statistics/details?servicearea=Mobiltjenester&label=Maskin-til-maskin%20-%20omsetning

PTS also collects data on the amount of revenue generated by M2M subscriptions. On a per subscription basis these have declined since 2008, decreasing from a little more than USD 2 per month in 2008-09, to roughly USD 1 in 2016 (Figure 9). A further Nordic communications authority collecting data on M2M revenues is in Norway where the experience has been similar to Sweden, as monthly revenues per M2M subscriptions have declined over the past three years. This may be because of the large increase in M2M devices and new tariff plans.

Although OECD countries have witnessed high growth of M2M connected devices, in terms of revenues, M2M is still a nascent market. For instance, according to PTS, M2M only generated USD 106.05 million in revenue in 2016, making up 1.7% of the total Swedish telecommunication market. Nevertheless, M2M as subset of IoT has the potential to grow in the near future with new business cases emerging. Although at present M2M is not large in terms of revenues, with the growth of IoT and evolving business models, it is expected to become the majority of connections with implications for infrastructure with the advent of 5G and autonomous vehicles.

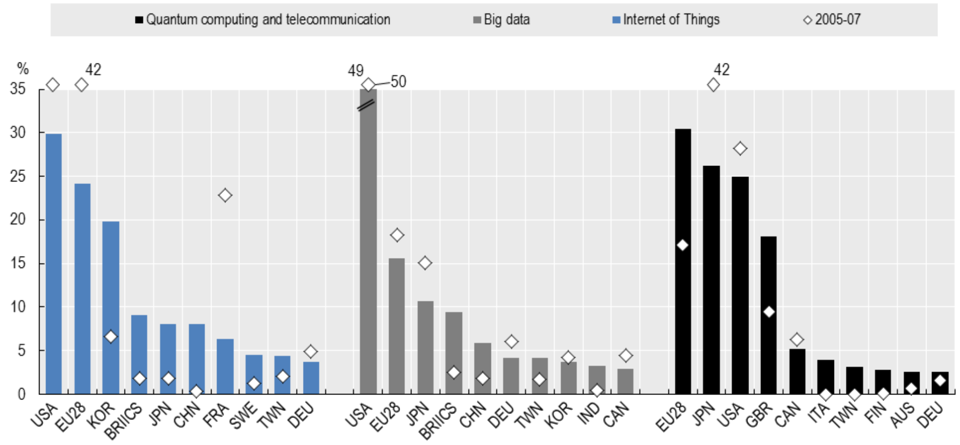
4.4. Other Government Agencies measuring IoT

4.4.1. Intellectual Property Offices definitions

The OECD 2015 Scoreboard published IoT patent information based on work done by experts from the United Kingdom Intellectual Property Office (IPO) (Figure 10). The IPO in its report "*Eight Great Technologies: A summary of the series of patent landscape reports*" mapped inventive activity regarding ICT disruptive technologies over the period 2004-13 by analysing patent documents published worldwide.

Figure 10. Top players in IoT, big data and quantum computing technologies, 2005-07 and 2010-12

Economies' share of IP5 patent families filed at USPTO and EPO, selected ICT technologies.



Note: Data refer to IP5 patent families with members filed at the EPO or the USPTO, by first filing date and according to the applicant's residence using fractional counts. The Intellectual Property Office (IPO) of the United Kingdom has allocated patent documents to technology fields. For further details on IPO's patent landscape reports on Eight Great Technologies (October 2014), see www.gov.uk/government/publications/eight-great-technologies-the-patent-landscapes.

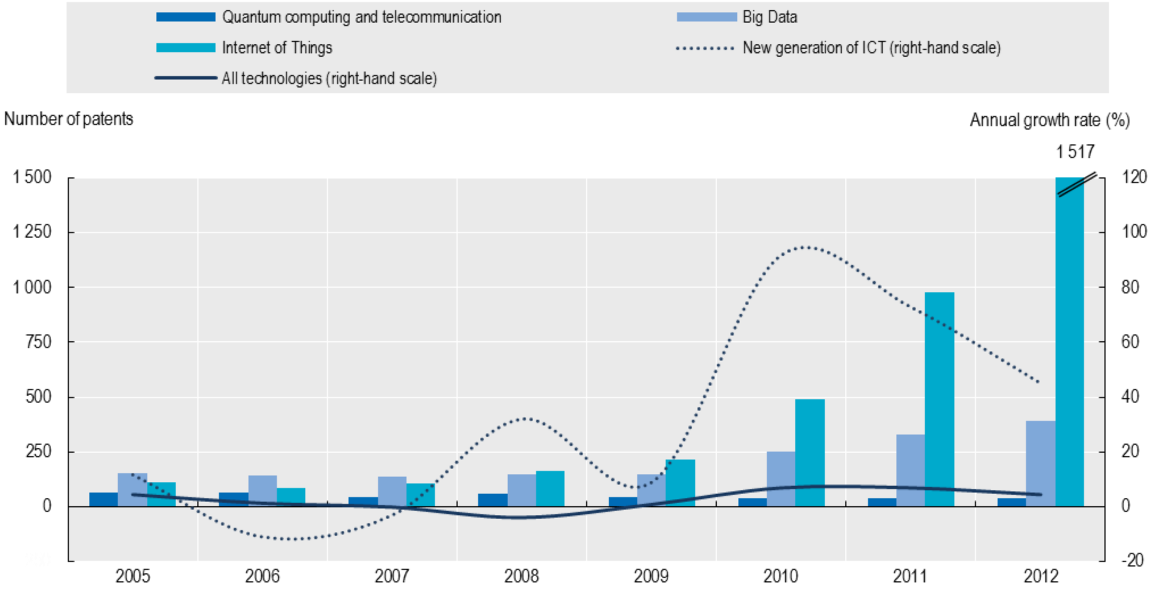
Source: OECD calculations based on IPO (2014), Eight Great Technologies: the Patent Landscapes, United Kingdom and STI Micro-data Lab: Intellectual Property Database, http://oe.cd/ipstats, June 2015.

The IPO spotted enabling technologies that form the basis of the new generation of ICTs: quantum computing and telecommunication, the Internet of Things, and big data. The definition of the Internet of Things (IoT) in this document is, "*networks of everyday physical objects that can be accessed through the Internet and are able to automatically identify themselves to other devices. Examples include remote control appliances, traffic congestion optimisation, e-health and industrial auto-diagnosis*" (IPO, 2014[27]). European countries --especially the United Kingdom--, were found to have led developments in quantum computing, whereas the United States were found to have led developments in both IoT and big data-related technologies (OECD, 2015[28]).

Patent activities related to the Internet of Things (IoT) grew throughout 2005 to 2012. In 2012, the annual growth rate of IoT reached 126% (Figure 11) (OECD, 2015[28]).

Figure 11. Patents in new generation of ICT-related technologies, 2005-12

Number of IP5 patent families and annual growth rates.



Note: Patent data refer to IP5 patent families by first filing date. The Intellectual Property Office (IPO) of the United Kingdom has allocated patent documents to technology fields. For further details on IPO's patent landscape reports on Eight Great Technologies (October 2014), see www.gov.uk/government/publications/eight-great-technologies-the-patent-landscapes.

Source: OECD calculations based on IPO (2014), Eight Great Technologies: the Patent Landscapes, United Kingdom and STI Micro-data Lab: Intellectual Property Database, http://oe.cd/ipstats, June 2015.

The United Kingdom IPO report on IoT

Within the disruptive technologies covered, the IPO published a special report on IoT called "Eight great technologies: The Internet of Things". This report states that from 2004 up until 2013, the worldwide dataset contained almost 22 000 published IoT patents (i.e. 10 000 patent families). The patenting of IoT related elements has been rapidly growing with an average CAGR of 40% between 2004 and 2013 compared to an average 6% increase across all technologies. In addition, more that 75% of IoT patent families were first filed in China, the United States or Korea (IPO, 2014).

According to this IPO (2014) report, the company that had filed more IoT patents by 2014 was the Chinese firm ZTE, mostly related to M2M communication, vehicle automation, and IoT security recognition. LG and Samsung had also IoT patents related to data transmission and storage, but at that point in time, were more interested in smart homes. Up until 2013, the media had reported much interest in IoT by firms like Apple and Google. However, Apple was ranked 27 in the list of top IoT applicants, and Google 84th. However that year Google acquired Nest Labs who specialised in Smart Homes (IPO, 2014[29]).

It is possible to display the subgroups of IoT, or the technology breakdown of the IoT Patent Families found in this IPO report (Table 2). The subgroups are based on the International Patent Classification (IPC). The largest proportion of IoT patents filed during 2005-13 relates to M2M technologies, and the second largest refers to smart meters (IPO, 2014[29]).

Table 2. The International Patent Classification (IPC)* subgroups of IoT Patent Families

H04L29/08	Communication control; Communication processing -> characterised by a protocol -> Transmission control procedure, e.g. data link level control procedure
H04L12/28	Data switching networks -> characterised by path configuration, e.g. LAN (Local Area Networks) or WAN (Wide Area Networks)
H04L29/06	Communication control; Communication processing -> characterised by a protocol
G06F15/16	Digital computers in general; Data processing equipment in general -> Combinations of two or more digital computers each having at least an arithmetic unit, a programme unit and a register, e.g. for a simultaneous processing of several programmes
G05B19/418	Programme-control systems -> electric -> Total factory control, i.e. centrally controlling a plurality of machines, e.g. direct or distributed numerical control (DNC), flexible manufacturing systems (FMS), integrated manufacturing systems (IMS), computer integrated manufacturing (CIM)
H04W84/18	Network topologies -> Self-organising networks, e.g.ad hoc networks or sensor networks
H04W4/00	Services or facilities specially adapted for wireless communication networks
G08C17/02	Arrangements for transmitting signals characterised by the use of a wireless electrical link -> using a radio link
H04W72/04	Local resource management, e.g. selection or allocation of wireless resources or wireless traffic scheduling -> Wireless resource allocation
H04B7/26	Radio transmission systems, i.e. using radiation field -> for communication between two or more posts -> at least one of which is mobile

Note: *The IPC provides for a hierarchical system of language-independent symbols for the classification of patent applications according to the different areas of technology to which they relate. However, the classifications are not mutually exclusive and each patent family may have several classifications applied.

Source: The Intellectual Property Office (IPO) of the United Kingdom (IPO, 2014) patent landscape report: *Eight Great Technologies: The Internet of Things* (August 2014), see https://www.gov.uk/government/publications/new-eight-great-technologies-internet-of-things.

4.4.2. The European Conference of Postal and Telecommunications Administrations (CEPT)

The ECC, within the CEPT, has published a report on “Numbering and Addressing in Machine-to-Machine (M2M) Communications” with the aim of helping NRAs when considering numbering and addressing solutions for M2M applications. The CEPT defines M2M as “*a communication technology where data can be transferred in an automated way with little or no human interaction between devices and applications*” (CEPT, 2010[30]).

In 2010, the CEPT reached four important conclusions. First, based on their analysis, they projected that the expected annual growth rate required for M2M numbers during 2010-20 was approximately 20%. They also highlighted that in the long run IPv6 addressing will become a key alternative to numbering resources, at least for a part of the M2M applications. They also mentioned that a significant number of CEPT countries did not have enough capacity in their numbering plan to accommodate the growth of M2M. Finally, they made a call for a harmonised approach on possible numbering solutions in Europe (CEPT, 2010[30]).

4.5. ICT usage surveys in OECD countries

From a demand side perspective, recent or forthcoming ICT usage surveys for businesses, households and individuals include a limited number of questions related to IoT. The related questions, in detail, can be found in Annex C.

Regarding surveys for households and individuals, the questions are generally limited to selected household smart appliances[14], health or wearable devices[15], or Cloud storage services (Table 3).

Table 3. IoT related question in the ICT usage survey questionnaires: selected recent examples for households and individuals

Items	Australia	Canada	Eurostat	Japan	Korea	Mexico	United States
Household equipment and appliances	2014-15 2016-17	2018	2014 2016 2019	2015 2016	2017	2016	2017
Wearable devices				2016	2016 2017		2017
Health		2018					
Cloud			2014-17	2015 2016	2015 2016	2016	2017

Note: See detailed questions in Table A C.1 of Annex C.
Source: Own elaboration, compiled from Eurostat and national sources.

With regard to business surveys, RFID and Cloud services have been tracked for several years (Table 4). IoT devices, Smart devices, or sensors have been introduced more recently in these surveys, though to date employed relatively infrequently (e.g. on big data usage, or about the perception of digital technologies, and so forth).

Table 4. IoT related question in the ICT usage survey questionnaires: selected recent examples for businesses*

Items	Australia	Canada	Eurostat	Japan	Korea
RFID	2015-16	2014	2011 2014 2017	2014 2016	2014-16
IoT, Smart devices, sensors	2015-16	2014	2016 2018	2014 2016	2015-16
Cloud services	2014-16	2012	2014 2016 2017	2010-16	2012-16

Note: *All are ICT surveys, except for Canada (i.e. advanced technology survey). See detailed questions in Table A C.2 of Annex C.
Source: Own elaboration, compiled from Eurostat and national sources.

Eurostat is specifically planning to introduce a question in the Community Survey on ICT Usage in households and by individuals 2019 Questionnaire, as follows: "*Did you use the internet for interacting with household equipment or appliances that are connected to the Internet, such as connected thermostat, light bulb or security system, in the last 3 months?*"

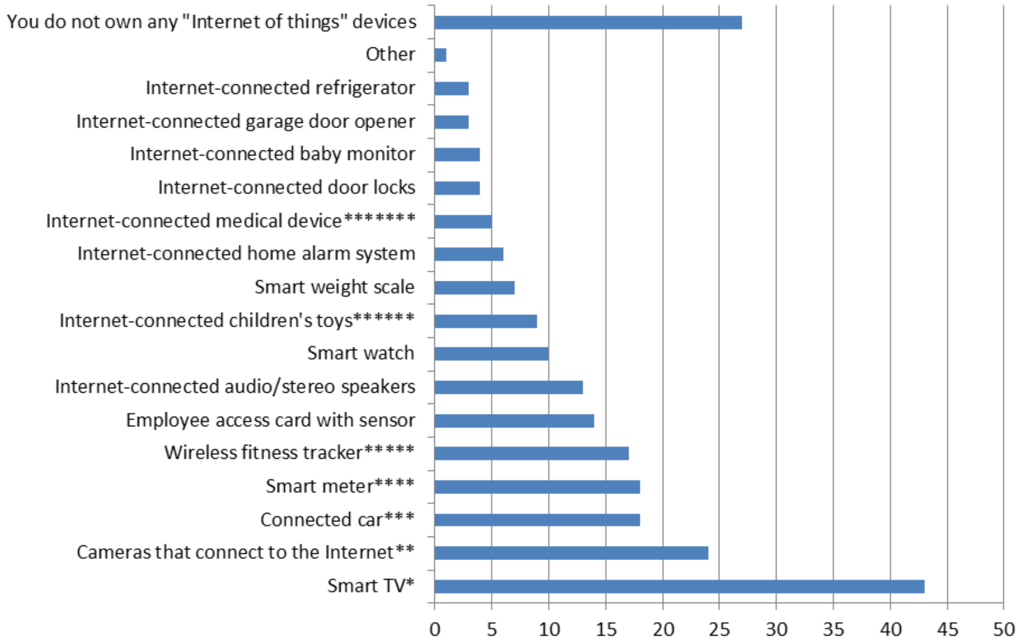
A more comprehensive set of questions on the Internet of Things is planned for the 2020 Eurostat Questionnaire. The wording of the 2019 Eurostat question is close to that developed by the NTIA in the United States (NTIA, 2017[31]).[16]

4.5.1. Other survey sources: Information Systems Audit and Control Association (ISACA)

A number of surveys are beginning to be conducted on the ownership and use of the IoT. ISACA, for example, surveyed 1 000 individuals in the United Kingdom in 2016 (Figure 12)

Figure 12. Ownership of Internet of Things devices in the UK 2016, by type

Share of the types of Internet of Things (IoT) devices owned in the United Kingdom (UK) in 2016.



Note: *e.g., Apple TV, Samsung Smart TV), **e.g. Wi-Fi-enabled video or digital cameras than can directly upload photos to the internet/cloud, ***e.g. car with Internet connection, GPS system or electronic toll collection device, ****e.g. an internet-connected thermostat or utility meter, *****e.g. Fitbit, Fuel Band, ******e.g. Wi-Fi-connected toys that can record and talk to children and may feature microphones, cameras, speakers and motors, *******e.g. heart monitor.
Source: ISACA, August 12, 2016 to August 23, 2016.

However, due caution needs to be observed in surveys given the novel nature of the IoT and that some applications may not be recognised by users. For example, a survey of 3 700 drivers in Europe conducted in 2015 found that 39% of automobile owners were unaware that their cars were "connected vehicles" (TNS and Bearing Point, 2016[32]). Even if the remaining 60% of automobile owners were aware they purchased a connected vehicle, they may not know that their car may have multiple SIM cards (i.e. one for the entertainment system and one for telemetry). The natural question that arises from a metrics perspective is how to account for this device. Is it two M2M connected devices in the case of having two SIM cards or a single subscription?

A further question that arises with regards to consumer wearable devices is how to count connected devices. In other words, what is the role of new embedded SIM cards wearables, which, according to CISCO, already accounted for 11 million devices in 2016? This raises the question of whether a consumer responding to a survey is aware that their device has an eSIM as opposed to a regular SIM card. It further raises the question of the implication of this type of SIM cards when measuring M2M connected devices. For example, in the case of the Apple Watch Series 3, the eSIM technology inside it is associated to a mobile communications plan. Finally, this raises the question of whether this wearable will be accounted for as a mobile device or as an M2M connection.

4.6. Mapping IoT

A further way to measure the IoT is through what are called IoT search engines, such as Thingful or Shodan, which scan the world of connected devices on the Internet and index them. That is, these search engines ping connected devices that are “openly available”, and geo-locate them. The way they categorise the devices as being environmental sensors or others, depends on the definitions they establish in their programming codes.

4.6.1. Thingful

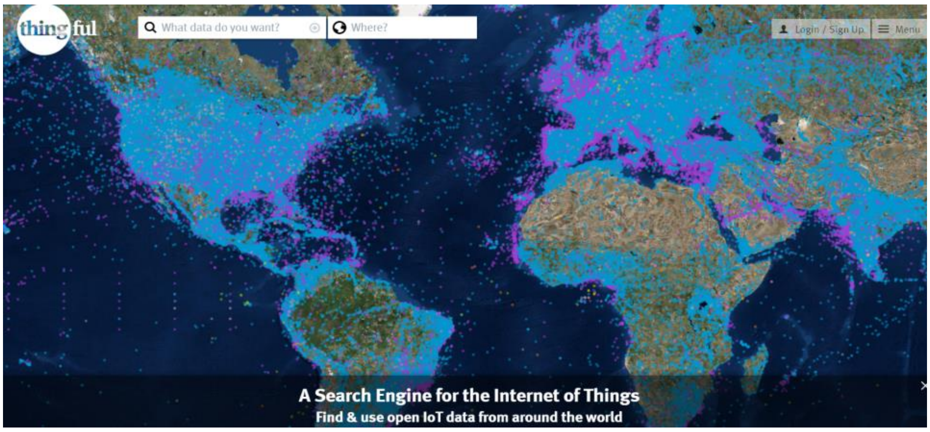
Thingful describes itself as a search engine for the Internet of Things, and provides maps of discoverable connected devices that are “openly available”, meaning that they have adequate data ownership certificates. Broadly speaking, they only index resources that:

- generate time-series data that updates at least once a day
- have a single geolocation
- have a unique URL or identifier where they can be accessed.

The Thingful definition of a “connected device” is, “A generic IoT device that generates a set of measurements. The measurements could be directly from physical sensors or by calculation.” Their definition of a connected vehicle is “a vehicle that is equipped with Internet access, and usually also with a wireless local area network. This allows the vehicle to share Internet access with other devices both inside as well as outside the vehicle.”

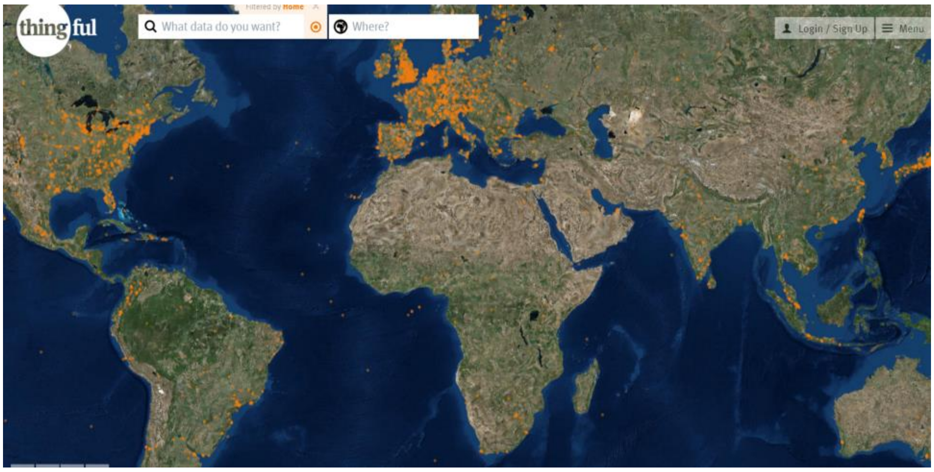
Following their definition for connected devices, Thingful can display those detected in a particular region or on a map of the world (Figure 13). The different colours that can be observed in Figure 13 indicate categories of connected devices. These “device categories” include: 1) energy (e.g. thermostat, electric meters), 2) health (e.g. Fitbit, heart monitors), 3) home, 4) flora, 5) environment (e.g. air quality sensors), and 6) transport (e.g. ships, vessels, trucks, automobiles). An example can be displayed here for devices found under Thingful’s categorisation for home devices across part of the globe (Figure 14).

Figure 13. Thingful IoT Map



Source: www.thingful.net

Figure 14. Thingful map of IoT home devices



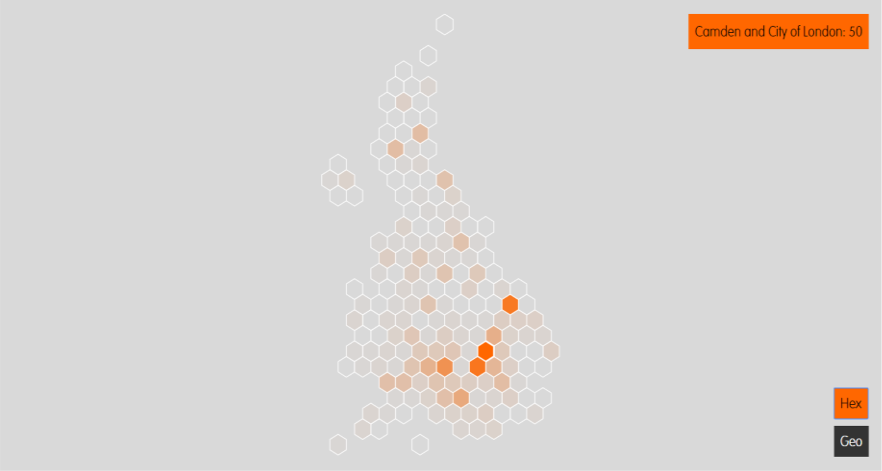
Source: www.thingful.net

4.6.2. IoTUK Nation Database

The IoTUK Nation Database brings together a snapshot of businesses and organisations comprising the IoT sector in the United Kingdom by using open data to bring together and cross-reference information from a variety of sources. To illustrate where organisations are located, they created a hexagonal "heat-map" representation of regions, where the stronger the colour of a hexagon is, the more organisations are in that region (IoTUK Nation, 2017[33]). In the Camden and City of London region, for example, this approach found 50 IoT organisations (Figure 15).

Figure 15. IoTUK Nation "heat map" of IoT firms

Example: Camden and City of London region.

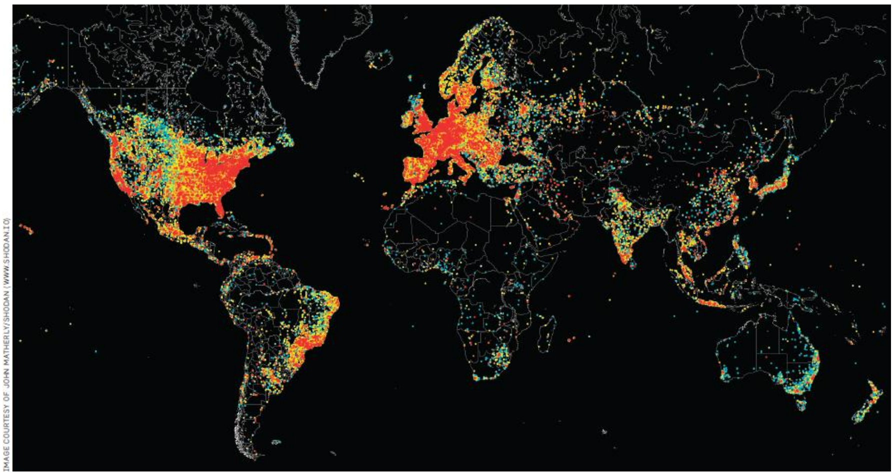


Note: The hexagonal representation of regions aims to give the same visual weight to areas with roughly similar populations (150 000 – 800 000).
Source: https://odileeds.org/projects/iot/

4.6.3. Shodan, a search engine for the IoT

Shodan was launched in 2009 as a search engine for connected devices. Currently, Shodan crawls nearly four billion devices over the IPv4 network, as well as a number of IPv6-connected devices (Alex Wright, 2017[34]). Unlike web browsers that use Hypertext Transport Protocol (HTTP), Shodan surveys other TCP/IP-connected ports including FTP, SSH, SNMP, SIP and RTSP ports in search of responsive servers (Alex Wright, 2017[34]). When it receives a welcome message, (or a "ping" as expressed by Shodan), the search engine retrieves the metadata of the connected device which can then be mapped (Figure 16).

Figure 16. Shodan Map of the IoT



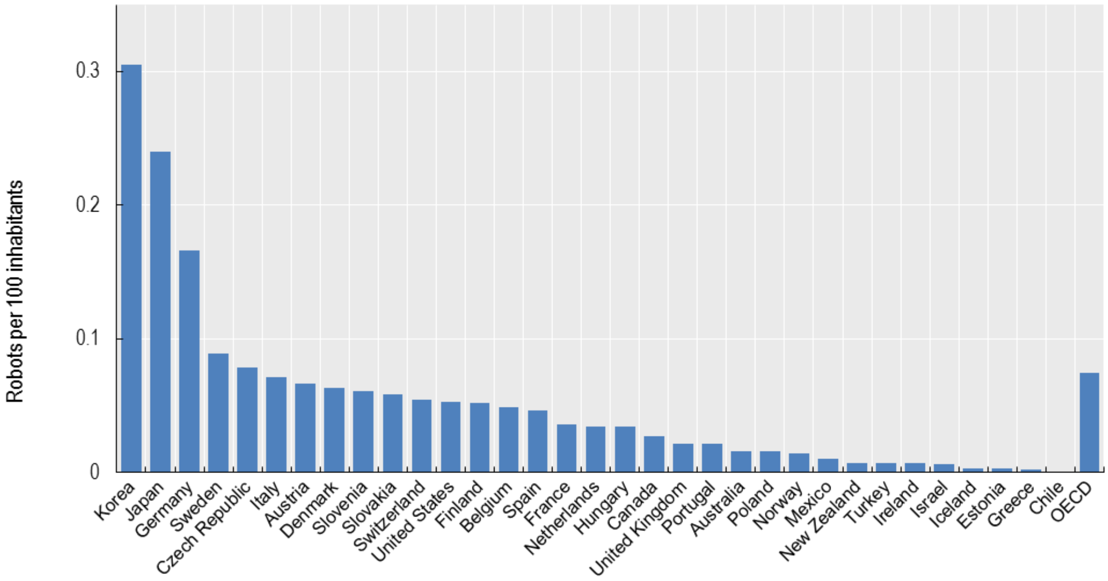
Source: www.shodan.io

4.7. IoT and Robots: future measurement area

Data are available on the degree of penetration of robots across OECD countries (Figure 17).The International Federation of Robotics (IFR) collect these data and the dataset is built by consolidating information from almost every industrial robot supplier in the world, and has been used by the OECD for some time.[17] The IFR data contains a measure of robot stock across roughly 100 geographic locations and industries from 1993- 2015 (OECD, 2017[35]).

At present, the IFT data on robot deployment does not include the number of connected robots. The IFT does, however, plan to begin collecting these data from 2018. This could provide a valuable set of data for this category of IoT connectivity.

Figure 17. Robot penetration OECD countries, 2015



Note: 2013 instead of 2015 for Finland and Slovenia.
Source: International Federation of Robotics (IFR).

4.8. IoT and the Environment: M2M sensors and smart meters

Massive M2M communication services comprised the vast amount of sensors that will be used in cities (e.g. electrical grids and highways), in industry (e.g. sensors within machines), as well as in the agricultural sector (e.g. sensors measuring humidity levels to improve water efficiency or better predict crop yields).[18] One characteristic of this type of M2M devices is that their deployment will be massive in the sense that they are millions of dispersed sensors in wide areas (in terms of km). However, the amount of data transmitted per device may be smaller (compared to IoT critical applications), and they tend to be less sensitive to latency issues.

There has been some measurement of sensors in terms of “smart meters”. A recent report from the Environment Directorate of the OECD on smart meters and consumer behaviour highlighted that the rollout of smart meters to residential customers is underway in many countries of the world (Table 5). By 2016, for example, in Canada and the United States, approximately half of all residential meters have been replaced by smart meters.[19] This report says, however, that in the United Kingdom and France, the rollout of smart meters to households lags behind North America (Rivers, 2018[36]).

Table 5. Residential smart meter rollout in selected countries and regions

Region	Number of residential Smart meters	Number of residential Accounts	Smart meter penetration	Year
France	1 500 000	29 000 000	5%	2016
Germany	1 600 000	40 000 000	4%	2014
Italy	26 000 000	26 000 000	100%	2015
Ontario, Canada	5 000 000	5 000 000	100%	2016
United Kingdom	3 500 000	27 000 000	13%	2016
United States	57 107 785	131 864 192	43%	2015

Note: Data from France: metering.com, https://www.metering.com/reports/linky-smart-meter-enedis/; *Germany:* Zhou and Brown (2017); *Italy*: Uribe-Pérez et al. (2016); *France, Italy, Germany* (number of households): Eurostat (2016); *Ontario:* Office of the Auditor General of Ontario (2014); *United Kingdom*: Department for Business, Energy and Industrial Strategy (2016), Office for National Statistics (2016); *United States*: U.S. Energy Information Administration (2017).

Source: OECD report "Leveraging the Smart Grid: The Effect of Real-Time Information on Consumer Decisions" (Rivers, 2018[36]).

A further environmental application that relies more and more on IoT, and in particular, in the use of massive and disperse sensors, is Smart Livestock Farming (SLF). The latter refers to the use of Information and Communication Technologies (ICT) applied into livestock value chains to boost productivity in the agricultural sector by integrating different processes such as Precision Livestock Farming (PLF), Management Information Systems (MIS), agricultural automation and robotics. The integration of all these processes aims to improve management and decision-making. In this sense, the IoT used for SLF aims at providing a full coverage of the processes by collecting and transmitting data from the entire agro-ecosystem. That means SLF can establish contact with each participant of a livestock chain, gathering information about their processes and, increasing the possibilities for control and improvement on the efficiency of their tasks. In terms of measurement of these devices, the question remains if it would be better to contact the owners of the SLF to get indicators, or the connectivity providers of such systems.

5. Do some categories of IoT devices require prioritising in terms of measurement?

5.1. Will some IoT devices, such as automated vehicles, generate large increases in demands on infrastructure?

While ‘connected cars’ have been commonplace for several years, the increasingly emerging levels of driver autonomy are likely to make new demands on communication infrastructures. Fully automated vehicles, sometimes called driverless or autonomous vehicles, generate very large amounts of data, thus raising questions such as the following:

- How much data will be generated by a fully automated vehicle?
- How much of this data transmission needs to be in real time?
- How much of this data is on-net and off-net?
- Over what distance will data need to be transmitted for vehicle-to-vehicle or other communication?
- How much data will need to be uploaded and downloaded when a vehicle is stationary such as in a garage with a fixed broadband connection?

The data transmission requirements of fully automated vehicles may have strong implications for network infrastructure, and therefore require prioritisation in terms of measurement in order to track developments. At the same time, the exponential growth of data requirements in automated vehicles may present considerable policy challenges (i.e. security, safety, privacy, and so forth) that may be explored in future OECD work.

Prior to having a closer look at these different aspects, some overall remarks with regard to terminology regarding fully automated, autonomous, connected cars can be useful:

- Autonomous driving is based on the use of sensors and radar in the car itself (i.e. the car works “autonomously”).
- Connected driving uses connectivity and supports autonomous driving. The major part of connected driving uses ITS (i.e. short-range technology) which establishes vehicle-vehicle communication, and connectivity of the vehicle with road infrastructure. In the case of vehicles connected to mobile networks, it is only for special “added value” features of the car such as telematics and “infotainment” (i.e. security relevant driving features do not depend on mobile connectivity in this case).
- Automated driving describes the fact that the driver is getting less and less involved in the driving process

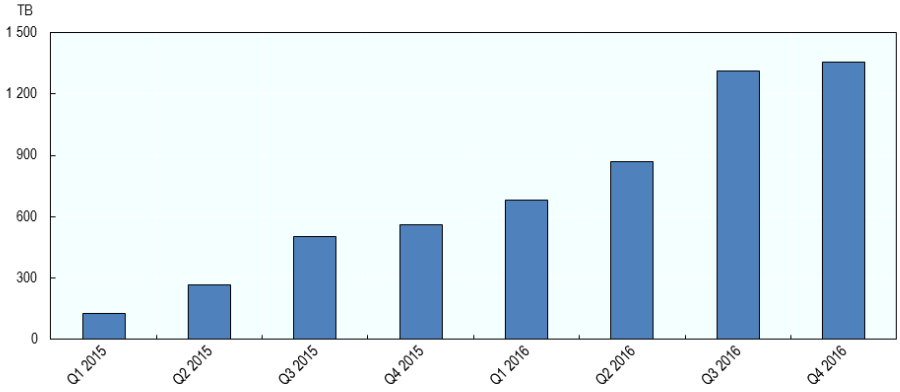
5.1.1. How much data?

There are different estimates for how much data a connected car will generate in the future and how much of these data will actually be transferred via telecommunication networks. The projections differ, perhaps due to definitions or expected technological developments. Nonetheless, all the estimates for connected cars are that they will produce a very large amount of data compared to today’s vehicles.

At present, Chevrolet connected vehicles in the United States used 4 220 684 gigabytes (GB) of data in 2016, an increase of nearly 200% with respect to 2015 (Chevrolet Media, 2017[37]). Just Tahoe and Suburban owners used 713 669 GB of data in 2016, which is equivalent to approximately 3 million hours of video streaming, or 1.8 billion songs, game or app downloads (Chevrolet Media, 2017[37]). That is, summing up quarterly data from the company, on-board data usage in Chevrolet connected vehicles grew from 1 455 terabytes (TB) in 2015 to 4 224 TB in 2016 (Chevrolet, 2016[38]) (Figure 18). To respond to the growing demand, in May 2017, AT&T introduced the "unlimited 4G LTE data plan" for connected vehicles, such as for Chevrolet owners, priced at USD 20 per month, with the caveat that after 22 GB of use AT&T may slow down the speeds (Chevrolet Media, 2017[39]).

Figure 18. On-board usage of data in connected Chevrolet vehicles

Data usage per quarter: Q1 2015-Q4 2016.



Note: TB = Terabyte.
Source: Chevrolet (2016), "Chevrolet lowers 4G LTE data pricing up to 50 percent", http://media.chevrolet.com/media/us/en/chevrolet/home.detail.html/content/Pages/news/us/en/2016/jun/0629-onstarData.html.

According to the head of marketing at Tuxera, a company that produces file management including for vehicles, a new 2017 car will generate about 20 GB of data every day, assuming the car has two cameras, 16 sensors and is driven one -two hours a day (Seminconductor Engineering, 2017[7]). In addition, according to Intel, the estimate is 4 000 GB per day. Not all these data, of course, need to be transmitted, which is an important factor when thinking about the requirements of networks to adapt to this exponential growth of data.

According to Barclays' analyst Brian Johnson, a single fully automated vehicle (i.e. level 4/5 of automation) --given all its sensors, cameras and LiDAR--, could generate as much as 100 GB of data per second (CNBC Autos, 2017[6]). In addition, this same Barclays' report mentioned that in the United States alone, "*260 million cars will produce about 5 800 Exabyte's of data daily, enough to fill 1.4 million Amazon tractor-trailer mobile data centres—or a convoy 11,000 miles long*" (Automobile Mag, 2017[40]).

A connected vehicle today has one or more SIM cards related to telematics (sensor data on the car's maintenance) and to "infotainment" (i.e. for the car's entertainment system using a Wi-Fi hotspot and 4G connectivity). While the amount of data generated by connected vehicles, or their users, is rapidly increasing not all the data needs to be transmitted in real time. Moreover, use by individuals of an on-board connection may be less than for a smartphone, especially given that a smartphone may be carried through work and leisure time whereas the time spent in a vehicle may be far less. In the near future, however, fully automated vehicles are expected to generate far larger amounts of data.

According to Intel, by 2020 the average internet user will produce 1.5 GB per day, whereas an autonomous vehicle will generate 4 000 GB of data per day (Figure 19) (Intel, 2016[5]). In other words, a single automated vehicle in a single day will produce data equivalent to around 2 700 Internet users. The connection speed requirements for a fully automated vehicle are made up of the following features: around 10-100 Kbps for the radar[20] and an equivalent amount for the sonar, approximately 50 Kbps for the GPS, around 10-70 Mbps for the LiDAR- the laser remote sensing system,[21] and 20-40 Mbps for the cameras. The total data generated is 4 000 GB per day, each day for each autonomous vehicle (Intel, 2016[5]).

Figure 19. Amount of data generated by an Autonomous Vehicle: Intel

Source: Intel, https://www.networkworld.com/article/3147892/internet/one-autonomous-car-will-use-4000-gb-of-dataday.html

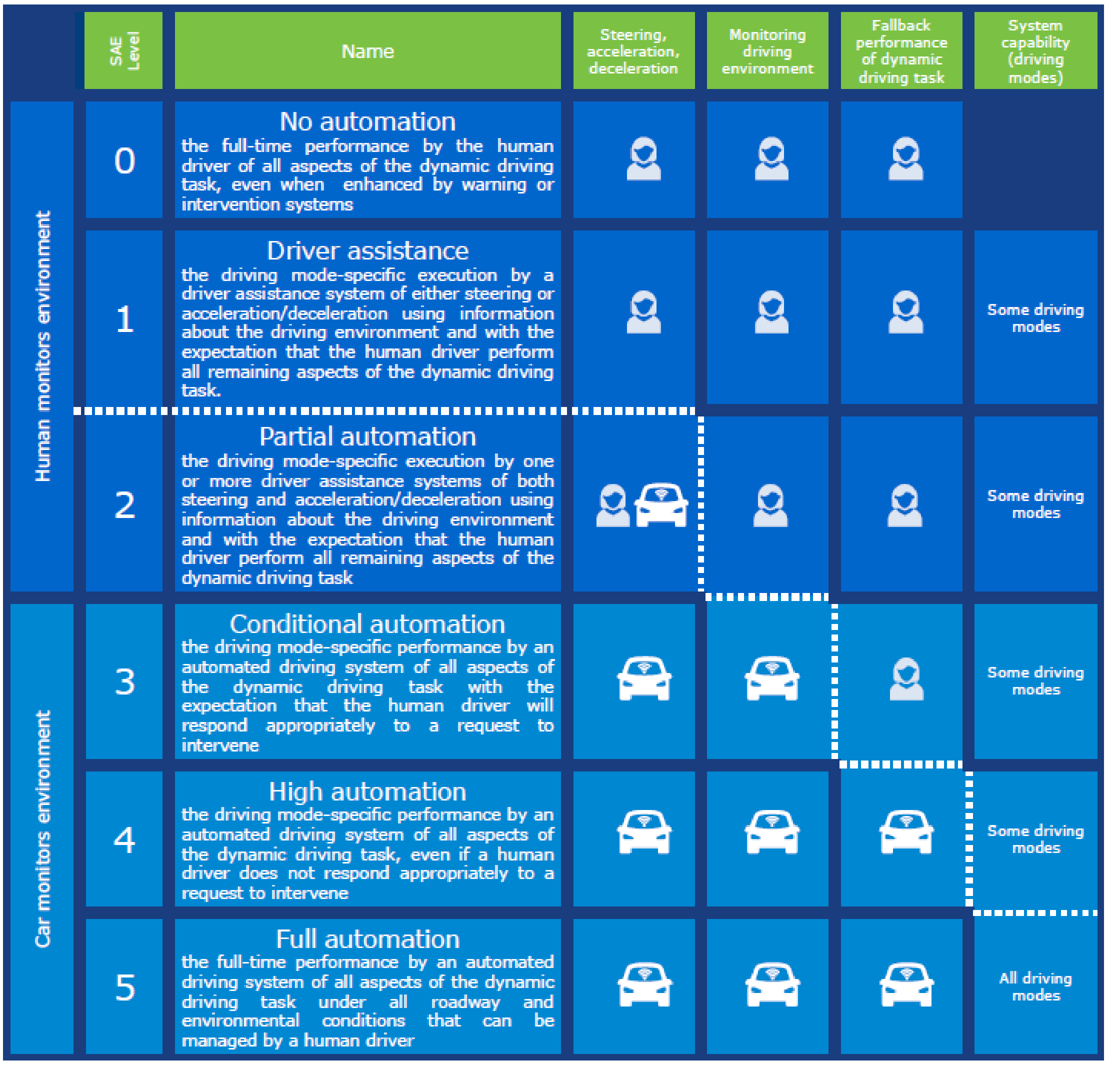
Meanwhile, according to Google Cloud, autonomous vehicles can produce upwards of 560 GB per vehicle, per day (Google Cloud Platform, 2017[41]). Many automobile manufacturers are engaged in tests in order to figure out, among other things, what are the data requirements for automated vehicles to work, as well as what regulatory requirements need to be adapted for automated vehicles to become a reality. For instance, in Sweden, Volvo is planning to offer customers fully automated vehicles by 2021, and initiated in January 2017 a trial of 100 self-driving vehicles tested by people drawn from the general public in the city of Gothenburg (Nordic Business Insider, 2017[42]). A further example is a recent research project in France currently devoted to benchmark 64 tests of connected and automated vehicles (CAV) around the world. One of the goals of this project is to quantify the different tests (number of vehicles in use and budget size). The results have not yet been published (TEVAC, 2017[43]).[22]

In terms of collecting the data of connected and automated vehicles, this could be done in several ways. One option could be with specific surveys addressed to the supply side (i.e. vehicle manufacturers). Other options could be to collect data from vehicle registries that exist in all countries, or by those providing connectivity, or perhaps even insurance companies. Most likely, each of these stakeholders will provide a different nature of indicators. For example, while the connectivity provider may have an idea of the amount of data traffic used per vehicle, the vehicle registries would only know the amount of connected vehicles by their model.

5.1.2. Will different levels of automation require different levels of connectivity?

One open question is whether the amount of data will depend on the degree of automation? To address this question, it is useful to review the levels of automation as defined by the Standard J3016 of the Society of Automotive Engineers. Under this definition, a human can intervene up to level three of automation (Figure 20).

Figure 20. Levels of automation according to the Society of Automotive Engineers



	SAE Level	Name	Steering, acceleration, deceleration	Monitoring driving environment	Fallback performance of dynamic driving task	System capability (driving modes)
Human monitors environment	0	**No automation** the full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems	👤	👤	👤	
	1	**Driver assistance** the driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task.	👤	👤	👤	Some driving modes
	2	**Partial automation** the driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task	👤 🚗	👤	👤	Some driving modes
Car monitors environment	3	**Conditional automation** the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene	🚗	🚗	👤	Some driving modes
	4	**High automation** the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene	🚗	🚗	🚗	Some driving modes
	5	**Full automation** the full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver	🚗	🚗	🚗	All driving modes

Note: Figure from pg. 14 of "Automated and Autonomous Driving" (OECD/ITF, 2015[44]).
Source: Adapted from SAE Standard J3016 (SAE, 2014[45]).

Connectivity requirements may vary as a function of the level of automation of the vehicle. To this regard, a report by the International Transport Forum pointed out that: "*levels of automation beyond conditional automation (Level 3) may operate on the basis of inputs solely from vehicle-embarked [embedded] sensors (self-sensing) or via a combination of self-sensor input and inputs from sensors embarked [embedded] on other vehicles and infrastructure that are communicated to the vehicle to the vehicle in near real-time*" (OECD/ITF, 2015[44]).

Furthermore, the connected vehicle and connected infrastructure approach requires available data transmission frequencies, low-latency, trusted, secure and fail-safe data transmission protocols and harmonised data syntax that ensures safe interoperability (OECD/ITF, 2015[44]).

5.1.3. The nature of data traffic created by automated vehicles: more upstream or downstream data?

In 2017, AT&T had 14.6 million connected cars on its network, adding around one million more each quarter. At present, AT&T bi-furcates the billing of data traffic for each automobile manufacturer using its network between telematics data and infotainment data connected. While today AT&T reports that most data from these connections are related to entertainment, they believe this trend will be reversed once cars are fully automated.

According to Sandvine, a company that tracks data usage among a panel of fixed broadband users in North America, real-time entertainment accounted for over 71% of downstream bytes during peak periods in 2016, which represented a slight increase with regards to the 70% reported in 2015 (Sandvine, 2016[46]). At the time, Sandvine reported that the use of Netflix accounted for the largest proportion of downstream traffic (i.e. 35%), with 17.53% for YouTube. While patterns for mobile usage may differ from fixed networks, they are also believed to generally involve more data being downloaded than uploaded. This raises the question of whether IoT will reverse this trend. That is, will the prevalence of IoT and automated vehicles create more upstream data than downstream traffic?

5.1.4. What data or applications are more sensitive to latency issues?

Some of the data used by automated vehicles may be extremely time-sensitive (i.e. real time decisions that must be made by the fully automated car while in traffic in a matter of milliseconds). Other applications within connected or autonomous vehicles will not be as sensitive to time or latency issues (i.e. telematics sensor data for vehicle maintenance). For data that is not required immediately by an automated vehicle, it may still be very valuable for other reasons. For example, some data on road conditions, such as wear and tear, may be useful for road maintenance. These data could be uploaded when a vehicle was parked or garaged and therefore use a fixed network. Likewise, software updates for a vehicle, if not time sensitive, could occur at the same time. That being said, even fixed networks would experience a large increase in demand for traffic if substantial proportions of the data generated by automated vehicles need to be uploaded.

Other examples of data that may be sensitive to latency issues, but do not require real-time transmission (therefore are not sensitive to time), are some products found for smart cities. For example, AT&T not only has endeavours in the connected vehicles area, but also has a product for smart cities. In their experience, some nodes (with many sensors connected to them) in a smart city may carry data, which is not time sensitive, but would be very sensitive to latency issues. A notable example is the real time transmission of data to analyse traffic patterns by cameras in street lamps. While they may be able to download the data during off-peak hours, the footage has to be reliable and in order to be so it requires minimal latency.

5.1.5. How are car manufacturers addressing the exponential increase in data?

Automobile manufacturers are building data centres and embracing new digital strategies and tools to meet the large growth expected in terms of data generated by increasingly automated vehicles, to produce better products and services and perhaps with an eye to issues around data ownership. By way of examples, Volkswagen is exploring quantum computing, and BMW is building a data centre near Munich ten times the size of the company's existing facility (NYT, 2017[47]). In the United States, Ford has announced a USD 200 million investment to build a new data centre in Flat Rock, Michigan, as it expects a 1 000% increase in data usage due to the necessary connections between automotive and computing technologies in a partially and fully automated vehicle world (DataCenter Knowledge, 2017[48]).

Many automotive companies are turning to develop in-house strategies to face the computing, analytics and data storage challenges for driver-less vehicles to become a reality. For example, Bosch will invest USD 1.1 billion in a new factory to produce chips for a variety of applications, including sensors in self-driving vehicles (NYT, 2017[47]). BMW is also reportedly developing digital capabilities in house and uses artificial intelligence to analyse the vast amount of data generated from the test-driving of automated vehicles. The company says that most data centres have to be on their own premises, as the amount of data is so large it cannot rely solely on cloud computing. On the other hand, Volvo has turned to outside providers such as Ericsson for computing technology, and will install Google's Android operating system in new cars as of 2019 (NYT, 2017[47]).

5.1.6. IoT Platforms for automated vehicles: data interoperability

New data streams are being generated in order to ensure vehicle-to-vehicle (V2V) communication, and vehicle-to-everything (V2X) communication. Different solutions are emerging requiring the co-ordination of multiple stakeholders through common platforms.

In an IoT platform for driverless vehicles, the challenge is to integrate many heterogeneous technologies that help the car navigate (Semiconductor Engineering, 2017[49]). IBM, for example, is developing a new IoT platform for autonomous vehicles that uses cognitive computing (IBM, 2017[50]). The IBM patent for this cognitive computing system helps determine if and when a person—or the self-driving system—should take control of the vehicle in order to prevent collisions (Popular Science, 2017[51]).

Collaboration among different stakeholders to build IoT platforms for automated vehicles is starting to increase. For instance, Intel first partnered a year ago with Mobileye, an Israeli company that makes cameras and sensors, and then acquired the company in March 2017 for USD 15.3 billion (Tech Crunch, 2017[52]). With this acquisition some suggest Intel wishes to become the leader of computing systems for automated cars (NYT, 2017[53]). More recently BMW and FIAT-Chrysler partnered with Intel (and with its acquired company Mobileye) with the aim of creating a technology platform for highly automated driving (Automotive News, 2017[54]).

5.2. What is needed in terms of infrastructure deployment (e.g. ITS, 5G)?

One of the current potential bottlenecks for IoT to become a pervasive reality, and for vehicles to become fully automated, could be related to network connectivity. An exponential increase of data generated by automated vehicles could represent challenges for the platforms that connect and manage this data. The implications and potential responses for any exponential increase of data will rely on the some of the following elements of communication infrastructure:

- 5G
- backhaul
- IXPs and data centres
- Cloud services.

An ideal IoT network solution would need to fulfil the following conditions: 1) wide coverage and connection of multiple devices, 2) low energy consumption, 3) low cost, and 4) reliable connectivity. In the subsequent paragraphs, the report will review some aspects of network connectivity that are important parts of the IoT ecosystem.

5.2.1. ITS

Automated and connected driving involves direct communication between cars or between cars and road infrastructure, which happens via ITS (Intelligent Transport System) technology, a short-range technology, rather than via mobile networks.

The European Commission promotes the use of a dedicated network, the C-ITS platform, for connected car services. In 2014, the European Commission decided to take a more prominent role in the deployment of connected driving, by setting up a C-ITS Deployment Platform. The Platform was conceived as a cooperative framework including national authorities, C-ITS stakeholders and the Commission, in view to develop a shared vision on the interoperable deployment of C-ITS in the EU. It shall provide policy recommendations for the development of a roadmap and a deployment strategy for C-ITS in the EU and identify potential solutions to some critical cross-cutting issues.

In the frame of supporting the deployment of C-ITS on European roads, there are a number of C-ITS real-life pilot projects funded under different programmes, which will create new ITS services for all European road users. These projects will test vehicle-to-infrastructure and vehicle-to-vehicle interactions by using both short-range and cellular communications.

5.2.2. Standardisation and 5G

One of the main challenges to be addressed with regards to IoT is to ensure a reliable connection that is interoperable with other IoT devices and networks. Mobile connectivity is but one type of connectivity used for IoT devices and networks. BEREC, found, based on data by Machina Research, that only a minor fraction of M2M connections will be based on cellular technologies, which means that some of the IoT devices may require a SIM card, but most of the IoT devices will not (BEREC, 2016[9]).[23] Other connectivity networks used are for example Low Power Wide Area Networks (LPWAN, please refer to section 5.2.3 below), or fixed networks.

With regard to mobile (cellular) connectivity used for IoT, a 5G standard holds the promise of becoming central to the IoT given its ability to bring together heterogeneous networks such as RFID and Bluetooth with cellular technology (5G Americas, 2017[55]). In addition, the fact that 5G will most likely use new spectrum in high frequency bands, makes it particularly appealing as an IoT solution (Fierce Wireless and TelecomAsia, 2016[56]).

Intel has expressed the view that for autonomous vehicles to become a reality, data flows in and out of such cars should be done at faster rates than today's LTE mobile networks. Thus, Intel has pointed out that 5G networks may become the "oxygen" for fully automated vehicles (VB, 2017[57]).

BMW has pointed out that one of the main challenges for autonomous driving is that in order to process all the data gathered by sensors, wireless networks need to be further advanced including with 5G. They say that for Level 5 automated vehicles (i.e. fully autonomous vehicles), with at least 33 sensors ranging from scanners to LiDARs, 5G networks will need to be in place by 2020 (BMW Blog, 2017[58]). They note that fully autonomous driving requires downloading very detailed maps in real time, and BMW believes this would require 5G connectivity. Furthermore, connectivity may be important for security reasons and this may be time sensitive. By way of example, BMW says their vehicles need to be connected to a back-end so that in the event of a security attack or vulnerability being detected, an encryption update can be automatically provided on more that 10 million vehicles within 24 hours (CarAdvice Australia, 2017[59])

The key characteristics of 5G will be the following (3GLTEinfo, 2015[60]):

- connection speeds up to 20 Gbps (compared to maximum 1 Gbps achieved with LTE today),
- coverage real speeds as experienced by users ranging from 100-1 000 Mbps (versus 10 Mbps in 4G networks),
- latency of 1 millisecond (ms) (as opposed to 10 ms in 4G), and
- device connections of 200 000 devices/km2.

With growth of the IoT, the 5G standard will have to address a wide range of applications with distinct network requirements. The 5G standard holds the promise of addressing the adaptability the network will require for each of these applications (Ericsson, 2017[4]). As mentioned previously, Ericsson has highlighted that automated vehicles will require low latency (i.e. lower than 5ms) and 100% network reliability and coverage, whereas massive dispersed connected M2M objects, such as sensors, will require 100% network coverage, a 10-year battery life but not be sensitive to latency (Ericsson, 2017[4]).[24]

Several 5G trials are occurring. For instance, Korea launched a 5G pilot network for the Pyeong Chang 2018 Winter Olympics in collaboration with Korea Telecom (KT), which displayed the world’s first testbed of the next generation of wireless communication services. This offered the opportunity to test 5G self-driving buses from the Seoul Airport to the Pyeong Chang Olympic campus, as well as self-operating 5G drones. In addition, SK Telecom has already tested its self-driving vehicle on the Gyeongbu Expressway in Korea, traveling 26 km at a speed of up to 80 km/hour, and plans to connect self-driving vehicles to its 5G trial networks (Telecom Lead, 2017[61]). Meanwhile in Europe the Republic of San Marino will have one of the first deployments of 5G with trials also underway in parts of Italy to highlight the potential for use in areas such as transport (Telecom Italia, 2017[62]).

In the future, automated vehicles making use of 5G networks may require the establishment of new partnerships among countries. In light of this need, in April 2018, a number of European countries signed agreements to establish cross-border 5G corridors for connected and automated driving. This builds up from existing agreements (signed in 2017) between 27 EC member states to conduct cross-border 5G trials (Mobile World Live, 2018[63]).[25]

5.2.3. LPWAN for IoT

The use of low power wide area networks (LPWAN) is a key aspect of the IoT infrastructure, and refers to a large number of low power devices located virtually everywhere. Wide area networking technologies are divided into two groups: a) a group focuses on unlicensed spectrum, such as LoRA and SigFox, and b) a group referring to connections operating within licensed spectrum, such as LTE- M and NB-IoT (MediaTek Blog, 2017[64]).

LPWAN technologies that rely on licensed spectrum are now being launched in many places around the world. In the United States, operators such as Verizon and AT&T have upgraded their LTE networks to support LTE-M services, and Deutsche Telekom and Vodafone have deployed NB-IoT in several European markets (GSMA, 2017[65]). In Korea, SK Telecom, KT and LGU+ have already started to use LTE-M in 2016 and in the first half of 2017, KT and LGU+ deployed NB-IoT. At the same time, SK Telecom deployed a LoRA network in June 2016.

Some say that 3GPP LPWAN technologies, such as NB-IoT and LTE-M are preferable to other existing LPWAN technologies such as LoRA and Sigfox, as they are easily scalable on existing 4G networks, and thus can reach more customers at a lower cost (MediaTek Blog, 2017[64]). GSMA notes that NB-IoT is the leading technology among the 4.5G or Advanced LTE alternatives (i.e. 3GPP) for IoT.

With regards to LPWAN, Korea has shared a table comparing LTE-M with LoRA networks (Table 6).

Table 6. Comparison of LTE-M and LoRA technologies, Korea

	LTE- M	LoRA
Advantages	Scalability from existing LTE networks	Non-expensive chips and modules
	Better QoS through licensed spectrum	Low energy consumption, and 10 year battery
	Standards already exist	Simple user interface
	Security as in LTE	Easy to install in mobile towers
Disadvantages	Expensive and complicated chips and modules	Need to deploy a new network
	High energy consumption devices	Relies on unlicensed spectrum
	Open service is complicated	Standardisation issues
	No business model so far	Chip ecosystem is limited

Source: Own elaboration based on NIA presentation on 5G and IoT.

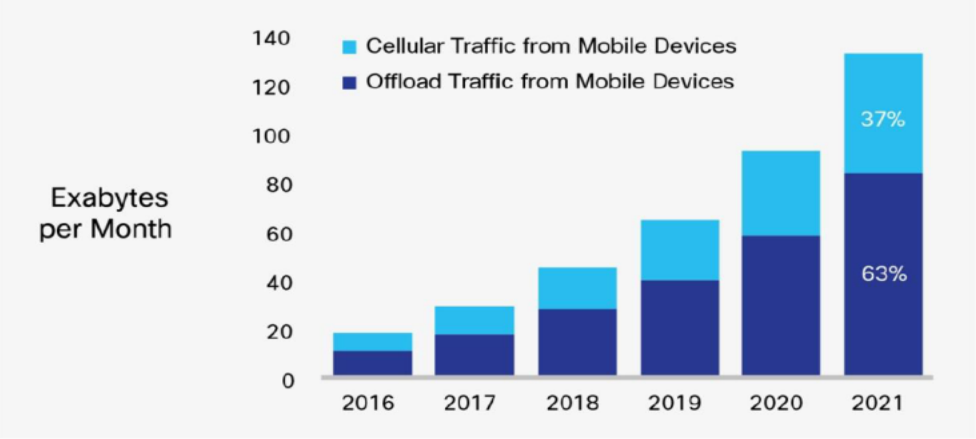
5.2.4. Cloud services

Cloud solutions are also seeking to help the flow of data generated by fully automated vehicles. In this respect, Google recently launched the “Cloud IoT Core” which is a computing platform “that takes advantage of Google’s end-to-end security model” (Google Cloud, 2017[66]). With the aim of building the foundation of vehicle-to-vehicle (V2V) communication, Google is designing a “Connected Vehicle Platform” using this “Cloud IoT Core” platform (Google Cloud Platform, 2017[41]).

5.2.5. Back to the basics: Fibre (backhaul)

Fixed and wireless networks continue to be highly complementary. By way of example, according to CISCO some 60% of mobile data was offloaded to fixed networks through Wi-Fi or femtocells in 2016, equivalent to 10.7 Exabytes per month (Figure 21) (CISCO, 2017[67]). This trend illustrates how the increase of data due to more IoT connected devices is likely to rely on more backhaul and backbone fibre connectivity.

Figure 21. Total Mobile Data Traffic offloaded to Wi-Fi Fixed Networks, CISCO



Note: Offload pertains to traffic from dual-mode devices (excluding laptops) over Wi-Fi and small cell networks.
Source: CISCO VNI (2017).

A recent study by Deloitte pointed out that for the case of the United States, fixed broadband access supports as much as 90% of wireless traffic (Deloitte US, 2017[68]). As such, they argue that much of the success of 5G in the United States will ultimately depend on fibre deployment. They concluded that an estimated USD 130-150 billion fibre investment is needed in order to meet future broadband needs (Deloitte US, 2017[68]).

As an example of the complementarities between fixed and wireless networks, the CEO of Verizon recently pointed out in an interview that his company is committed to redesigning its network to be “*from the cloud through high speed fibre infrastructure to edge computing to 5G*” (Seeking Alpha, 2017[69]). To do so, in addition to running 5G trials in 11 cities, they are investing in deploying 12.5 million miles of fibre per year for the next three years (Seeking Alpha, 2017[69]).

6. Emerging regulatory and policy challenges related to the IoT highlighting the importance of measurement

Together with the benefits IoT may deliver, new policy and regulatory challenges may emerge in some areas (e.g. privacy/security concerns, as well as interoperability, numbering and standardisation issues). Thus, creating indicators to inform policy making in these areas, is a priority. Although the primary scope of the present report is examining measurement of the IoT, it is worth mentioning areas for future work, as well as to recall previous OECD work on IoT.

Previous OECD work has highlighted, among other regulatory issues, numbering, addressing and interoperability for the IoT. Thus, in order to foster the IoT ecosystem, interoperability, spectrum management, extra-territorial use of numbers, and solutions to facilitate provider switching as to avoid lock-in become crucial. Furthermore, previous work has underscored the importance of IPv6 as a key enabler of the IoT (OECD, 2016[1]).

In addition to questions about interoperability, numbering and other standards, there is a need to build privacy, security, liability and reliability around the use of the IoT. For example, potential liability issues require a clear identification of responsibilities particularly when a malfunctioning device can have negative social or economic outcomes (OECD, 2016[1]).

Developing metrics on digital security, in general, is a relatively complex task and still an emerging measurement area for the IoT. This means there is merit for future work focusing on statistics on security standards and practices surrounding the IoT including at the OECD. Measurement to inform policy makers in these areas is likely to gain in importance, as there will be a need for interoperability of policy frameworks across borders and sectors. This will be at the forefront in areas such as consumer protection, safety, privacy and security, particularly when products are designed, manufactured and sold in countries with different approaches (OECD, 2016[1]).

7. Concluding remarks

7.1. Suggested criteria for IoT measurement

As IoT devices increasingly become IP based and platform-agnostic (i.e. operating on mobile, fixed, and other networks), demand has grown for approaches that measure the number of such devices and to improve the understanding of their implications for telecommunication networks. The current OECD working definition of IoT provides a framework to guide policy discussions and could be rendered more useful by adding subcategories for measurement purposes.

7.1.1. General principles when establishing priorities in terms of measurement and collecting IoT data

Given its vast nature, some categories of IoT devices require prioritising in terms of measurement. When establishing priorities in terms of measurement, policy relevance and feasibility can be among the main considerations when making the choice.

A notable IoT application that will likely require prioritisation in terms of measurement are automated vehicles, as they will generate very large amounts of data, likely having an important influence on communication infrastructure. In this sense, measurement of automated vehicles becomes crucial from city planning perspective, for environmental considerations, for transport ministries, and for communication regulators, among others.

The practicalities associated with collecting data for IoT indicators needs to be taken into account. A key factor for measurement, where there are several stakeholders in supply chains involved, is to keep in mind the ownership of the data.[26] Another relevant consideration is the regulatory burden imposed when collecting the data, and how feasible (and reliable) is that process. In particular, measuring IoT may be especially complicated for devices using unlicensed frequency bands, as there are no administrative authorisation or declaration procedures in these bands. In all these considerations policy makers should prioritise and have a clear objective for the data collected.

Additional aspects to be considered in relation to the measurement of the IoT:

Measuring “connected devices” by features:

- dispersion or concentration of devices/applications
- mobility of objects (stationary or nomadic),
- data volume and network performance (bandwidth)
- sensitivity to latency.

Categorising IoT by technological options for their use and adoption:

- sensors and simple hubs
- integrating hubs (i.e. a system that connects simple hubs creating more complex devices such as Apple’s HomeKit)
- enhanced applications (i.e. services that collect and analyse data from connected devices and the environment in real time such as “automated vehicles”).

Taking into account the underlying IoT infrastructure that enables communication among devices:

- Cloud services
- quantum and edge computing,
- data storage
- mobile networks
- LPWA networks
- backhaul and backbone connectivity, and so forth.

7.1.2. IoT measurement in ICT usage surveys by firms, households and individuals

From a usage perspective, as IoT is of an evolving nature where the types of connected devices are rapidly changing, one of the difficult issues is to remain technology neutral. Another difficulty relies in the awareness of consumers of the connected nature of the devices they own.

An option when conceiving IoT related questions to be included in household and firm surveys is to measure the progression of connected devices among a "generic" family of objects (e.g. home appliances, wearable devices) or more complex goods (e.g. cars, trucks, tractors). This can be done from the producer perspective (using statistics from associations or from specific supply side surveys) or from the user perspective (e.g. by developing ad-hoc modules in ICT usage surveys).

The categories of devices according to application domains (e.g. home or health) could be implemented in modules within ICT household and Individuals usage surveys. It is, therefore, very welcome that Eurostat will add an IoT related question (similar to that included by the United States) in its 2019 ICT household survey. As well, Eurostat's current consideration to add a module on IoT for the household usage surveys is timely. On the other hand, the interaction of IoT devices with the business processes could be better-measured using specific modules to be implemented within ICT firm usage surveys.[27]

7.2. Proposal of an OECD definition and taxonomy of IoT

The proposal set out here is to endorse the current OECD working definition of IoT, by excluding devices that are already taken into account in OECD metrics (i.e. smartphones, tablets and PCs), and adding subcategories for measurement purposes. The breakdown of IoT into several subcategories such as "Massive Machine to Machine communications" (e.g. sensor like M2M), and critical IoT applications (e.g. automated vehicles) appears to be a reasonable way forward in order to create measures of IoT that are adequate to inform policy making.

The overarching IoT definition would be:

> *"The Internet of Things includes all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals. While connected objects may require the involvement of devices considered part of the "traditional Internet", this definition excludes laptops tablets and smartphones already accounted for in current OECD broadband metrics."*

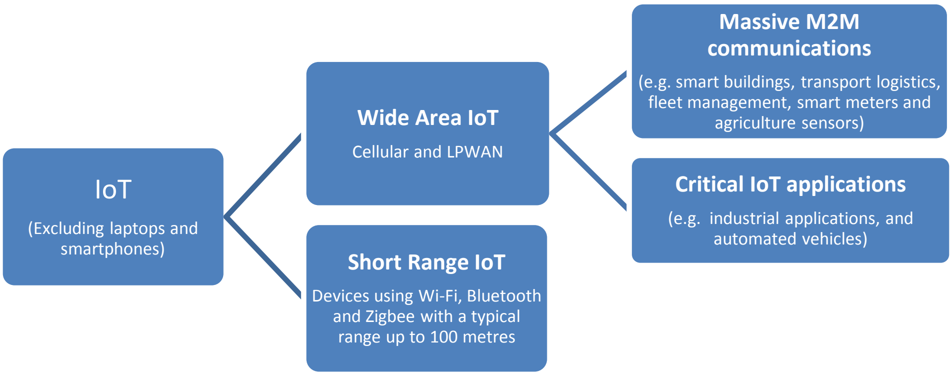
The benefits of restating the OECD definition and complementing it by adopting subcategories are manifold. Namely, two main benefits are highlighted here. One, it renders the issue of measuring the IoT more tractable, and two, it allows for prioritisation in data collection in certain categories (or subcategories) of IoT that may have more influence on future demands in communication infrastructure.

The subcategories of IoT should be coherent with policy purposes, as well as IoT market developments. It is therefore natural to draw analogies the concepts set forth by the ITU in their vision of the fifth generation of wireless networks, or the IMT 2020 standard, yet to be finalised in 2019 in the ITU's World Radio Communications Conference (ITU, 2015[70]). This standard is being conceived with IoT in mind with three main usage scenarios: enhanced mobile broadband, massive machine type communications, and critical communications/applications.

Furthermore, taking into account these subcategories (e.g. massive machine type communications and critical IoT), would be in line with what several authorities in OECD countries have highlighted (e.g. France, Japan, Korea and Portugal), and consistent with the way other stakeholders developing the IoT business cases are currently measuring the IoT (e.g. Ericsson and CISCO).

Thus, the proposal is to divide IoT with the following subcategories in mind (Figure 22):

Figure 22. Proposed taxonomy of IoT for measurement purposes



Source: Own elaboration.

As noted previously, M2M communications constitute a subset of the IoT. Since 2012, with the object of teasing out the number of M2M subscriptions from the mobile voice subscriptions, the OECD has measured M2M embedded SIMs defined as "*the number of SIM-cards that are assigned for use in machines and devices (cars, smart metres, consumer electronics) and are not part of a consumer subscription*". A similar exercise has been undertaken when it comes to the measurement of IoT in broader sense. That is, OECD countries have opted to disentangle laptops and smartphones (already part of OECD's measurement) when creating indicators for the subcategories of IoT.

The two categories of IoT proposed are Wide Area and Short Range IoT. The Wide Area IoT category includes devices connected through cellular technology (NB-IoT or LTE-M) as well as those connected through Low Power Wide Area Networks (e.g. SigFox and LoRa networks), whereas the Short Range IoT category includes devices using unlicensed spectrum with a typical range up to 100 metres. In addition, the Short Range IoT refers as well to devices connected over fixed-line Local Area Networks (or LANs) and powerline technologies. It should be noted that this category may also include some M2M devices in smart buildings, logistics or industrial applications.

Within the category of Wide Area IoT, two subcategories are suggested: Massive M2M devices (e.g. sensors for agriculture or smart cities), and Critical IoT applications (e.g. remote surgery applications, fully automated vehicles and other industrial robotics applications). The reason for making the distinction between these two last subcategories of connected devices relies on the fact that critical IoT applications will have very different network requirements (i.e. high reliability and low latency), whereas massive and disperse M2M sensors may not be that sensitive to latency or high speeds of connectivity.

The main advantage of the proposed taxonomy is the simplicity to cover IoT applications in licensed spectrum provided by cellular network operators, as well as devices or applications rolled out by commercial LPWAN providers in order to be able to collect the data from these in a later stage for measurement purposes. However, a caveat for this definition and framework is that it may not provide a holistic view of the entire market and some private networks may be beyond the scope of the definition.

7.3. Further measurement issues

This report proposes a taxonomy of IoT for measurement purposes. Nevertheless, several IoT measurement issues remain outstanding. For instance, how will the substantial increase expected from billions of connected devices affect infrastructure requirements? To answer this question the first step is a framework to assess the size of the subcategories of IoT, which was the aim of the present report. The list below illustrates some general questions that may inspire future discussions:

- While IoT data use (i.e. data traffic per device) has been relatively modest to date, how will the next-generation of applications, such as automated vehicles, industrial IoT devices and so forth, change the data use profile of these devices?
- For the categories of IoT that deserve special attention given their implications to infrastructure (e.g. automated vehicles), what are the best ways to collect the information that ultimately informs policy?
- Given that many applications of IoT use private networks, and thus might not appear in supply-side data (i.e. communication service providers data), what other sources of data collection for IoT exist?

A more extensive list of such questions that may lead future discussions can be found in Annex A.

Annex A. Main outstanding questions/issues regarding IoT measurement

The following list summarises the questions that have been reviewed in the present report, and is intended to foster future discussion among delegates.

General questions

- While IoT data use has been relatively modest to date, how are next-generation applications, such as autonomous vehicles, industrial IoT devices and so forth, expected to change the data use profile of these devices in the future? Will the exponential increase in data expected from billions of connected devices affect infrastructure requirements?
- If some categories of IoT deserve special attention given their implications to infrastructure (e.g. autonomous vehicles), what are the best ways to collect the information that ultimately proves necessary to inform policy? For instance, what is the best source to collect data on connected robots (e.g. the producers of robots or the suppliers of the connectivity)? Similarly, what is the best channel to gather information on autonomous vehicles (e.g. vehicle registries that exist in all OECD countries or the producers of those vehicles or those providing connectivity)?
- Given that many applications of IoT use private networks, and thus might not appear in supply-side data (i.e. communication service providers data), what other sources of data collection for IoT exist?
- Taking into account that many consumers may be unware of whether their devices are connected, are household surveys are reliable source for accounting for IoT devices? For example, do consumers know that their car is connected, and if so, how many SIM cards it has? Is a consumer responding to a survey aware that their wearable device has an eSIM as opposed to a regular SIM card?

Regarding the measurement of IoT/M2M data traffic flows:

- Will these data flows be measured over public networks (fixed and mobile)?
- Is the number of IoT/M2M SIM cards one factor (but only one among others) to estimate the data flows, at least for cellular networks?
- How shall SIM cards be treated which enable both IoT/M2M applications and Non-IoT/M2M applications over a unique SIM (e.g. consumer SIMs over which smart home applications are controlled)?
    - How is the double counting of SIMs (for IoT and non-IoT) to be avoided?

Specific questions on M2M metrics

- Are their categories of devices that use SIM cards that deserved being broken out in the data collected by authorities given the different demands they make on infrastructures?
- When a device, such as a smartphone, has multi-homing of connectivity (e.g. it is able to use LTE-M and LoRa networks), is there a double accounting of M2M devices that use SIM cards and are LPWA connected devices?
- As new technologies start to emerge, such as the eSIM (embedded SIM) in wearable devices, how should we take into account these new SIM cards in M2M measurement?
    - Should devices using eSIMs, such as Apple Watch 3, be considered as a single or multiple connections?

  - If such embedded devices are recorded as multiple connections, will this wearable device be accounted for as a mobile device or as an M2M connection?

Questions about fully automated vehicles

Fully automated vehicles, sometimes called self-driving, driverless or autonomous vehicles, generate very large amounts of data, thus raising questions such as the following:

- How much data will be generated by a fully automated vehicle?
- How much of these data will be transferred via communication networks?
- Over which type of communication network (e.g. ITS, cellular network, other) will these data be transferred and in which amount?
- What data or applications are more sensitive to latency issues? That is, how much of this data transmission needs to be in real time? How much of this data is on-net and off-net?
- Over what distance will data need to be transmitted for vehicle-to-vehicle or other communication?
- How much data will need to be uploaded and downloaded when a vehicle is stationary such as in a garage with a fixed broadband connection?
- Will different levels of automation require different levels of connectivity?

Other questions regard the infrastructure implications of data generated by fully automated vehicles:

- Over which type of communication network (ITS, cellular network, other) will connected vehicles rely on?
- Will fully automated vehicles rely on 5G connectivity?
- How much more fibre should be deployed?
- Standardisation issues and IoT platforms
- Cloud services and data centres

Questions related to economic outcomes of IoT in different sectors:

- IoT outcome indicators, as opposed to only process indicators, for example:
  - **Smart city indicators**:
    - Number or percentage of public transportation vehicles;
    - Number/Percentage of smart traffic light installed;
    - Number/Percentage of cities monitored by cameras;
  - **Health indicators**:
    - Patients with chronic diseases using IoT applications;
    - Savings by IoT applications in health units,
    - IoT health applications developed by country.
  - **Rural indicators**:
    - Percentage of rural areas using IoT applications for climate monitoring,
    - Numbers of rural equipment or tools (e.g. tractors) that are connected,
    - Disease and sanitation control in livestock farm;
    - Country innovation on agricultural sector;
  - **Industry indicators**:
    - Productivity increase by IoT applications on operations management and preventive maintenance.

Annex B. Selected examples of other IoT Definitions

The International Telecommunication Union (ITU) defined IoT as:

- "*The definition of IoT refers to "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies", and where the "thing" is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks*" (ITU, 2012[71]).

The European Commission in 2014, under the context of the study "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination" (European Commission, 2014[72]) mentions the following:

- "*The Internet of Things enables objects sharing information with other objects/members in the network, recognizing events and changes so to react autonomously in an appropriate manner. The IoT therefore builds on communication between things (machines, buildings, cars, animals, etc.) that leads to action and value creation*".

The United States Bureau of Economic Analysis of the United States Department of Commerce in a 2018 publication on the measurement of the Digital Economy defined IoT as:

- "*Internet-enabled devices like appliances, machinery, and cars with embedded hardware allowing them to communicate with each other and connect to the Internet*" (Barefoot et al., 2018[3]).

The United States International Trade Commission refers to IoT in the following way (United States International Trade Commission, 2017[73]):

- Page 14: "*The Internet of Things refers to digital technologies that include Internet-connected physical devices and sensors.*"
- Page 24: "*IoT refers to the ever -growing network of connected objects that are able to collect and exchange data via sensors and other devices*".

The United States Department of Defence uses in its documents the IoT definition by the Institute of Electrical and Electronics Engineers (IEEE) (United States Department of Defense, 2016[74]). The IEE definition, which makes a distinction of IoT in terms of the complexity of the environment where devices operate, is the following (IEEE, 2015[75]):

- Small Environment Scenario: "*An IoT is a network that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'Thing' can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything*".
- Large Environment Scenario: "*Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, programmability feature and are uniquely identifiable. The representation contains*

information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration."

The United States Government Accountability Office (US GAO) defined IoT in 2017 as:

- "*technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information. These "smart" devices are increasingly being used to communicate and process quantities and types of information that have never been captured before and respond automatically to improve industrial processes, public services, and the well-being of individual consumers*" (United States Government Accountability Office, 2017[76]).

In addition, the United States GAO has broken down IoT into ten domains (or markets/segments):

- wearables
- smart homes and buildings
- vehicles
- manufacturing
- supply chain
- agriculture
- healthcare
- energy
- environment
- and smart communities.

AIG and Consumer Electronics Association (United States):

- "*The 'Internet of Things' doesn't primarily rely on computers to exist. Rather, every object, even the human body, can become a part of IoT if equipped with certain electronic parts. Those parts certainly vary depending on the function the object is to perform, but they fall into two broad categories: 1.) the object must be able to capture data, usually through sensors; and 2.) the object must be able to transmit that data to anywhere else through the Internet. A sensor and a connection, therefore, are the two primary electronic 'parts' of an IoT object*" (AIG and Consumer Electronics Association, 2016[77]).

McKinsey in a report (2017) defined IoT as:

- "*the network of connected "smart" devices that communicate seamlessly over the Internet*" (McKinsey, 2017[25]).

The World Economic Forum in 2015 defined IoT as:

- "*A network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment*" (WEF, 2015[78]).

Annex C. Detailed questions related to IoT in the ICT usage surveys (Household and Individuals, Firms)

Table A C.1. IoT related questions in the ICT usage survey questionnaires

Selected recent examples of Household and Individuals surveys

Items	Australia[1]	Canada[2]	Eurostat[3]	Japan[4]	Korea[5]	Mexico[6]	United States[7]
Household equipment or appliances							
Interact via the internet with household equipment or appliances (such as thermostat, light bulb, robot vacuum or security system)			2019				
What about interacting with household equipment or appliances that are connected to the Internet, such as a connected thermostat, light bulb, or security system? (If needed) Do you use the Internet to interact with household equipment or appliances?							2017
Do you currently use any of the following Internet-connected smart home devices in your primary residence? [8]		2018					
Home appliances that can be connected to Internet				2016			
Cooking heater, refrigerator etc. Smart appliances that can be connected to the Internet				2015			
Smart TV at home (separated item)			2014, 2016		2017	2016	
How many Internet-connected TVs do you/ does your household use to access the internet at home?	2014-15 2016-17						
TV Box: [Do you/Does anyone in this household] use a smart TV, a game or video system, or another device that connects to the Internet and plays through a TV? Examples include an Xbox, Apple TV, PlayStation, Roku, or a Blu-Ray player that can access the Internet.							2017
Wearable devices							
[Do you/Does anyone in this household] use a wearable device that is connected to the Internet, such as a smart watch or fitness band? Examples include an Apple Watch, Fitbit, or Microsoft Band. (If yes & is multi-person household) Who is that?							2017
What kind of wearable devices do you have now? Band type (Fitbit); Watch type; Baby Child and Elderly Protecting/Tracking type; Clothes type; Accessory type; Glasses type;					2016, 2017		
Please select all functions of a wearable device you are using: making/receiving a phone call or sending/receiving a message by connecting with smartphone; searching for information using the Internet; health management by measuring metrics such as heart rate and calories burn; recording travel distance and path; guidance of direction; experience of virtual reality and augmented reality; location tracking and protection of young children and elderly.					2016, 2017		
In a wearable device, what function do you have the highest expectation for? Please choose one. See above functions + controlling home appliances like smart TV, etc.; controlling air-conditioning and heating.					2016		
Wearable terminals (such as glasses,)				2016			

Health							
Do you use an electronic health monitoring service that collects and sends data to your doctor or health care provider through the Internet? Examples include connected devices that monitor vital statistics, blood glucose levels, or blood pressure.							2017
During the past 12 months, which of the following activities have you performed using your smartphone? […] Fitness tracking or health […]		2018					
Cloud							
Using Internet as storage space to save files for private purposes			2014-2017	2015-16	2015-16	2016	

Note: (1) Australian Bureau of Statistics, Multipurpose Household Survey, MPHS 2016/17; (2) Canadian Internet Use Survey 2018, draft; (3) Eurostat, Community Survey on ICT usage in households and by individuals; (4) Communication Usage Trend Survey, Ministry of Internal Affairs and Communications, Japan; (5) Survey on the Internet Usage, KISA; (6) INEGI, Encuesta Nacional sobre Disponibilidad y Uso de TIC en Hogares, ENDUTIH 2016; (7) November 2017 CPS Computer and Internet Use Supplement, US Bureau of the Census; (8). Refer to the ownership of the following detailed list: Virtual assistants (e.g., Google Home, Amazon Echo); Video cameras (e.g., security cameras, Nest Cam, baby monitors); Door or window locks; Thermostats (e.g., Ecobee, Nest, Sensi); Plug-ins or lights; Large appliances (e.g., fridge, stove, dishwasher); Smart televisions; Other smart home devices (e.g., garage door opener, vacuum).

Source: Own elaboration, compiled from Eurostat and national sources.

Table A C.2. IoT related questions in the ICT usage survey questionnaires

Selected recent examples of Business Surveys

Items	Australia[1]	Canada[2]	Eurostat[3]	Japan[4]	Korea[5]
RFID					
The use of Radio Frequency identification technologies (RFID): ► refers to an automated identification method to store and remotely retrieve data using RFID tags or transponders ► includes the use of Near Field Communication (NFC) connectivity standard An RFID tag is a device that can be applied to or incorporated into a product or an object and transmits data via radio-waves. NFC enables communication between devices within short distance (approx.10 cm or less). [please add national examples] Does your enterprise make use of Radio Frequency Identification instruments for the following purposes? (Y/N) ► Person identification or access control As part of the production and service delivery process (e.g. monitoring and control of industrial production, supply chain and inventory tracking; service, maintenance or asset management, etc.) For product identification after the production process (e.g. theft control, counterfeiting, allergen information, etc.)			2017 2014 2011		
During the year ended 30 June 2016, to what extent were the following digital technologies important to this business? ► A small extent	2015-16				

► A major extent ► A moderate extent ► Not at all (i) Radio frequency identification devices […]					
Does your enterprise use or plan to use any of the following Advanced Material Handling, Supply Chain and Logistics Technologies? h. Radio frequency identification (RFID)		2014			
Has your company adopted the following systems and tools that use wireless communication technology? […] 1. RFID tags […]				2014 2016	
Did your business/organisation use RFID technologies as of December 31, 201x? + For what purposes was your business/organisation using RFID as of Dec. 31,201x?					2014 2015 2016
IoT, Smart devices, sensors					
During 2015, did your enterprise analyse big data from any of the following data sources? ► Enterprise's own data from smart devices or sensors (e.g. Machine to Machine -M2M-communications, digital sensors, Radio frequency identification tags RFID, etc.) (In the context of big data)			2016 2018		
During the year ended 30 June 2016, to what extent were the following digital technologies important to this business? ► A small extent ► A major extent ► A moderate extent ► Not at all (h) Internet of things (e.g. smart metering, digitally-networked physical devices or assets) […]	2015-16				
Does your enterprise use or plan to use any of the following Advanced Design and Information Control Technologies? [...] h. Wireless communications for production i. Sensor network and integration j. Computer Integrated Manufacturing (CIM) k. Automated systems for inspection (e.g., vision-based, laser-based, X-ray, high-definition (HD) camera or sensor-based) [...]		2014			
Does your enterprise use or plan to use any of the following Geomatics or Geospatial technologies? a. Geographic information systems (GIS) b. Global positioning system (GPS) (exclude personal use) c. Remote sensing (RS) d. Mobile device with geolocation capabilities e. Web or wireless sensors f. Spatial data infrastructure [...]		2014			
Indicate whether your enterprise uses these Nanotechnology applications. Indicate whether your enterprise develops or produces any of these Nanotechnology applications. [...] [ ]: Nanomaterials (includes organic and inorganic nanocomposites, nano-powders, nanoparticles, nano-coatings, carbon nanotubes) […]: Nano-devices, including sensors, Nanoelectromechanical systems (NEMS) and nano-enabled Microelectromechanical systems (MEMS)		2014			

[…]: Nano-electronics, including photonics, nano-optical devices, nano-optical sensors or nano-optical light emitters [...]					
Has your company adopted the following systems and tools that use wireless communication technology? […] 3. New network-enabled devices (network cameras, sensors, etc.) […]				2014 2016	
Did your business/organisation use IoT device and service as of December 31, 201x?					2015 2016
For what purposes was your business/organisation using IoT device and service as of Dec. 31,2014? 1) Improvement of employee productivity 2) Lowering the cost and of manpower and maintenance 3) Lowering the cost of operating the business/organisation Mark 4) Fortify the work environment and safety of data security 5) Expansion of new products and new services 6) Expansion of support on a national level 7) Other (Please specify) :					2015
For what purposes was your business/organisation using IoT device and service as of Dec. 31, 2015? What do you think of the effectiveness through the usage (or the usage in the future) of IoT equipment and service in your company (scale of effectiveness of usage ranging from "no effect" to "very effective" for the items below) 1) Cost cutting 2) Increase of efficiency 3) Increase of productivity and information sharing 4) Reinforcement of information security 5) Improvement of work environment 6) Expansion of new source of profit and the creation of product (service) 7) Other (Please specify) :					2016
For which of the following reasons did your business/organisation not use IoT services as of Dec.31, 2014? Mark all that apply. 1) Concern over security 2) Uncertainty regarding the earnings model 3) A lack of basic machinery for the usage of IoT devices and services (Connected devices. embedded sellSOfS, etc.) 4) Lack of manpower capacity for the usage of IoT devices and services 5) Lack of compatibility of existing products and services 6) Low relevance with your business/organisation 7) Other (Please specify):					2015
For which of the following reasons did your business/organisation not use IoT services as of Dec.31, 2015? Mark all that apply. 1) Burden of economical expenses 2) Consideration with the security 3) Complexity of service (technology) 4) Lack of capability of operation personnel 5) Insufficient compatibility 6) Insufficient basic equipment 7) Immature IoT market 8) Miscellaneous (please specify):					2016
Did your business/organisation plan to use IoT devices and services?					2015 2016
Cloud services					
Purchasing Cloud services	2014, 2016	2012	2014 2016 2017	2010- 2016	2012- 2016

Note: (1). ABS, Business Characteristics Survey 2015-16; (2) Statistics Canada, Advanced Technology Survey 2014,http://www23.statcan.gc.ca/imdb/p3Instr.pl?Function=assembleInstr&a=1&&lang=en&Item_Id=184557; (3) Eurostat, Community Survey on ICT usage and e-commerce in enterprises; (4) Communication Usage Trend Survey, Ministry of Internal Affairs and Communications, Japan; (5) Survey on the Information society, Ministry of Science, ICT and Future Planning and National Information Society Agency, Korea.

Source: Own elaboration, compiled from Eurostat and national sources.

References

3GLTEinfo (2015), *5G the Real Answer for Internet Of Things (IoT) Complexity - Why is LTE not Enough? | 3GLTEInfo*, 10 March 2015, http://www.3glteinfo.com/5g-for-internet-of-things/ (accessed on 05 October 2017). [60]

5G Americas (2017), *LTE to 5G: Cellular and Broadband Innovation*, http://www.5gamericas.org/files/6415/0282/1551/2017_5G_Americas_Rysavy_LTE_5G_Innovation__Final_for_Upload.pdf (accessed on 05 October 2017). [55]

AIG and Consumer Electronics Association (2016), "The Internet of Things: Evolution or Revolution? Part 1 in a Series", *Chief Economist*, https://www.aig.com/content/dam/aig/america-canada/us/documents/insights/aig-white-paper-iot-english-digital-brochure.pdf (accessed on 09 April 2018). [77]

Alex Wright (2017), *Mapping the Internet of Things*, http://dx.doi.org/10.1145/3014392. [34]

ARCEP (2016), *Livre blanc – Préparer la révolution de l'Internet des objets – ARCEP | IoT*, utorité de Régulation des Communications Électroniques et des Postes, Paris, https://iot.arcep.fr/2016/11/07/livre-blanc-revolution-iot-nov2016/ (accessed on 10 April 2018). [19]

AT&T (2017), *AT&T INC. 2017 Annual Report*, https://investors.att.com/~/media/Files/A/ATT-IR/financial-reports/annual-reports/2017/complete-2017-annual-report.pdf (accessed on 22 August 2018). [16]

Automobile Mag (2017), *The Big Data Boom | Automobile Magazine*, 10 October 2017, http://www.automobilemag.com/news/the-big-data-boom/ (accessed on 11 October 2017). [40]

Automotive News (2017), *Fiat Chrysler joins autonomous driving platform from BMW / Intel / Mobileye | EETE Automotive*, http://www.eenewsautomotive.com/news/fiat-chrysler-joins-autonomous-driving-platform-bmw-intel-mobileye (accessed on 03 October 2017). [54]

Barboutov, K. et al. (2017), *Ericsson Mobility Report 2017*, Ericsson, https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf (accessed on 21 September 2017). [14]

Barefoot, K. et al. (2018), "Working Paper: Defining and Measuring the Digital Economy", https://www.bea.gov/digital-economy/_pdf/defining-and-measuring-the-digital-economy.pdf (accessed on 10 April 2018). [3]

BEREC (2016), *BEREC Report on Enabling the Internet of Things*, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things) (accessed on 09 April 2018). [9]

BMW Blog (2017), *Level 5 Autonomous Technology Not Possible Yet, Claims BMW*, 5 October 2017, http://www.bmwblog.com/2017/10/05/level-5-autonomous-technology-not-possible-yet-claims-bmw/ (accessed on 06 October 2017). [58]

BNetzA (2017), "Numbering plan for mobile numbers", *Official Gazette No*, Vol. 14/16, https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/NumberManagement/MobileServices/Mobileservicees_Numbering%20Plan_2017.pdf?__blob=publicationFile&v=2 (accessed on 10 April 2018). [21]

BNetzA (2016), “Extra-territorial use of foreign International Mobile Subscriber Identities (IMSIs) in the Federal Republic of Germany for machine-to-machine (M2M) communications” 11, https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/NumberManagement/TechnicalNumbers/IMSI_Extra-territorial.pdf?__blob=publicationFile&v=2 (accessed on 10 April 2018). [88]

BNetzA (2016), “Numbering plan for International Mobile Subscriber Identities” 11, https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/NumberManagement/TechnicalNumbers/IMSI_NP.pdf?__blob=publicationFile&v=2 (accessed on 10 April 2018). [20]

BNetzA (2011), *Bundesnetzagentur Annual Report 2011*, https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/ReportsPublications/2012/AnnualReport2011pdf.pdf?__blob=publicationFile (accessed on 10 April 2018). [22]

BnetzA (2017), “Bundesnetzagentur Annual Report 2016 Markets in the digital revolution”, https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/ReportsPublications/2017/AnnualReport2016.pdf;jsessionid=71B763A1F8F7D99BBBCD9D876BA823FE?__blob=publicationFile&v=2 (accessed on 10 April 2018). [23]

CarAdvice Australia (2017), *BMW: Fully-autonomous driving technology not yet available*, http://www.caradvice.com.au/583583/bmw-fully-autonomous-driving-technology-not-yet-available/ (accessed on 06 October 2017). [59]

CCFA (2017), *L'industrie automobile française*, https://ccfa.fr/wp-content/uploads/2018/01/Analyse_Statistiques_2017_FR.pdf (accessed on 10 April 2018). [87]

CEPT (2010), *ECC REPORT 153 NUMBERING AND ADDRESSING IN MACHINE-TO-MACHINE (M2M) COMMUNICATIONS*, European Conference of Postal and Telecommunications Administrations (CEPT) , Luxembourg, http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP153.PDF (accessed on 09 April 2018). [30]

Chevrolet (2016), *Chevrolet Lowers 4G LTE Data Pricing Up to 50 Percent*, http://media.chevrolet.com/media/us/en/chevrolet/home.detail.html/content/Pages/news/us/en/2016/jun/0629-onstarData.html..html (accessed on 12 October 2017). [38]

Chevrolet Media (2017), *Chevrolet Offers More Options to Add Unlimited Data*, http://media.chevrolet.com/media/us/en/chevrolet/news.detail.html/content/Pages/news/us/en/2017/may/0511-data.html (accessed on 21 September 2017). [39]

Chevrolet Media (2017), *Chevrolet Owners Consumed 4.22 Petabytes of Data in 2016*, http://media.gm.com/media/us/en/chevrolet/news.detail.html/content/Pages/news/us/en/2017/feb/0203-onstar.html (accessed on 21 September 2017). [37]

China Mobile (2017), *China Mobile Corp. Limited Annual Report 2017*, https://www.chinamobileltd.com/en/ir/reports/ar2017/2017_20f.pdf (accessed on 22 August 2018). [18]

China Telecom (2017), *China Telecom Corp. Limited Annual Report 2017*, https://www.chinatelecom-h.com/en/ir/report/annual2017.pdf (accessed on 22 August 2018). [17]

CISCO (2017), *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2016-2021*, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf (accessed on 22 September 2017). [67]

CISCO (2017), *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper - Cisco*, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html (accessed on 22 September 2017). [15]

CISCO VNI (2017), *VNI Mobile Forecast Highlights for Sweden, 2016-2021*, https://www.cisco.com/assets/sol/sp/vni/forecast_highlights_mobile/#~Country (accessed on 10 October 2017). [86]

CNBC Autos (2017), *An 'ocean of auto big data' is coming, says Barclays*, CNBC Autos, https://www.cnbc.com/2017/04/26/an-ocean-of-auto-big-data-is-coming-says-barclays.html (accessed on 11 October 2017). [6]

DataCenter Knowledge (2017), *Ford Plans $200M Data Center in Anticipation of Connected Car Data Explosion | Data Center Knowledge*, 29 March 2017, http://www.datacenterknowledge.com/archives/2017/03/29/ford-plans-200m-data-center-in-anticipation-of-connected-car-data-explosion (accessed on 06 October 2017). [48]

Deloitte US (2017), *Deep fiber: The next internet battleground*, https://www2.deloitte.com/us/en/pages/consulting/articles/communications-infrastructure-upgrade-deep-fiber-imperative.html# (accessed on 05 October 2017). [68]

Ericsson (2017), *Ericsson White Paper: 5G Systems – enabling digital transformation*, https://www.ericsson.com/assets/local/publications/white-papers/wp-5g-systems.pdf (accessed on 06 October 2017). [4]

European Commission (2017), *Connectivity Reports: Digital Scoreboard | Digital Single Market*, https://ec.europa.eu/digital-single-market/en/connectivity (accessed on 14 November 2017). [12]

European Commission (2014), *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination | Digital Single Market*, https://ec.europa.eu/digital-single-market/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination (accessed on 09 April 2018). [72]

Fierce Wireless and TelecomAsia (2016), *Will 5G be the Answer to the Internet of Things?*, 2016, https://pages.questexweb.com/CES_FierceWireless_Breakfast_2016.html?ref=el (accessed on 05 October 2017). [56]

Fondation MAIF (2018), *Labellisation de confiance des objets connectés*, https://www.fondation-maif.fr/pageArticle.php?rub=1&id=407 (accessed on 10 April 2018). [85]

Google Cloud (2017), *Cloud IoT Core | Google Cloud Platform*, https://cloud.google.com/iot-core/ (accessed on 04 October 2017). [66]

Google Cloud Platform (2017), *Designing a Connected Vehicle Platform on Cloud IoT Core | Solutions | Google Cloud Platform*, https://cloud.google.com/solutions/designing-connected-vehicle-platform (accessed on 22 September 2017). [41]

GSMA (2017), *Mobile IoT - Internet of Things*, https://www.gsma.com/iot/mobile-iot-executive-summary/ (accessed on 05 October 2017). [65]

IBM (2017), *Connected Cars with IBM Watson IoT*, https://www.ibm.com/internet-of-things/iot-solutions/iot-automotive/connected-cars/ (accessed on 03 October 2017). [50]

IEEE (2015), *Toward a Definition of Internet of Things (IoT)*, https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (accessed on 09 April 2018). [75]

Intel (2016), *Data is the New Oil in the Future of Automated Driving | Intel Newsroom*, 15 November 2016, https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/ (accessed on 05 October 2017). [5]

IoTUK Nation (2017), *IoTUK Nation Database: IoT Sector Mapping*, https://odileeds.org/projects/iot/ (accessed on 22 September 2017). [33]

IPO (2014), *Eight Great Technologies - A summary of the series of patent landscape reports*, http://www.ipo.gov.uk/informatics (accessed on 21 September 2017). [27]

IPO (2014), *Eight Great Technologies: The Internet of Things*, http://www.ipo.gov.uk/informatics (accessed on 21 September 2017). [29]

IPUMS CPS (2018), *Current Population Survey*, https://cps.ipums.org/cps/compint_sample_notes.shtml (accessed on 10 April 2018). [84]

ISO (2018), *ISO/IEC JTC 1/SC 41 - Internet of Things and related technologies*, https://www.iso.org/committee/6483279/x/catalogue/p/0/u/1/w/0/d/0 (accessed on 09 April 2018). [10]

ITU (2015), *Recommendation ITU-R M.2083-0 (09/2015), 'IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond'*, https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf. [70]

ITU (2012), *Overview of the Internet of things*, https://www.itu.int/rec/T-REC-Y.2060-201206-I (accessed on 09 April 2018). [71]

Le Monde (2018), “Auto, maison, santé : les assureurs font entrer les objets connectés dans les foyers”, http://www.lemonde.fr/entreprises/article/2018/02/12/auto-maison-sante-les-assureurs-font-entrer-les-objets-connectes-dans-les-foyers_5255295_1656994.html#0wsY9duUA2qw7G74.99 (accessed on 10 April 2018). [83]

McKinsey (2017), *The future of connectivity: Enabling the Internet of Things | McKinsey & Company*, https://www.mckinsey.com/global-themes/internet-of-things/our-insights/the-future-of-connectivity-enabling-the-internet-of-things (accessed on 09 April 2018). [25]

McKinsey Global Institute (2015), *Unlocking the potential of the Internet of Things | McKinsey & Company*, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (accessed on 21 September 2017). [13]

MediaTek Blog (2017), *MediaTek | Why NB-IoT is the best answer to the 5G LPWA future |...*, https://www.mediatek.com/blog/why-nb-iot-is-the-best-answer-to-the-5g-lpwa-future (accessed on 05 October 2017). [64]

MIC (2017), *Information and Communications in Japan 2017*, http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2017/2017-index.html (accessed on 10 April 2018). [24]

Mobile World Live (2018), *EU countries strike cross-border 5G agreements - Mobile World Live*, https://www.mobileworldlive.com/featured-content/home-banner/eu-countries-strike-cross-border-5g-agreements/?ID=003w000001z7mMOAAY&utm_source=sfmc&utm_medium=email&utm_campaign=MWL_20180410 (accessed on 11 April 2018). [63]

Nordic Business Insider (2017), *Volvo just launched the world's most ambitious autonomous driving trial in Gothenburg - Business Insider Nordic*, http://nordic.businessinsider.com/volvo-just-launched-the-worlds-most-ambitious-autonomous-driving-trial-in-gothenburg-2017-1 (accessed on 04 December 2017). [42]

NPR (2018), *National Public Media The Smart Audio Report from NPR and Edison Research*, https://www.nationalpublicmedia.com/smart-audio-report/ (accessed on 10 April 2018). [82]

NTIA (2017), *November 2017 CPS Computer and Internet Use Supplement*, the National Telecommunications and Information Administration (NTIA)., https://www.ntia.doc.gov/files/ntia/publications/november_2017_cps_supplement_draft_for_public_comment.pdf (accessed on 10 April 2018). [31]

NYT (2017), *BMW and Volkswagen Try to Beat Apple and Google at Their Own Game - The New York Times*, 22 June 2017, https://www.nytimes.com/2017/06/22/automobiles/wheels/driverless-cars-big-data-volkswagen-bmw.html (accessed on 03 October 2017). [47]

NYT (2017), *The Race for Self-Driving Cars - The New York Times*, 6 June 2017, https://www.nytimes.com/interactive/2016/12/14/technology/how-self-driving-cars-work.html (accessed on 03 October 2017). [53]

OECD (2017), *Industrial Robotics and the global organisation of production*, OECD, Paris, http://dx.doi.org/DSTI/CIIE(2017)14. [35]

OECD (2017), *The Next Production Revolution*, OECD Publishing, http://dx.doi.org/10.1787/9789264271036-en. [81]

OECD (2017), *The Next Production Revolution: Implications for Governments and Business*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264271036-en. [11]

OECD (2016), *Unclassified DSTI/ICCP/CISP(2015)3/FINAL Working Party on Communication Infrastructures and Services Policy THE INTERNET OF THINGS: SEIZING THE BENEFITS AND ADDRESSING THE CHALLENGES Background report for Ministerial Panel 2.2*, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En (accessed on 13 October 2017). [1]

OECD (2015), *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264232440-en. [89]

OECD (2015), *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264232440-en. [2]

OECD (2015), *OECD Science, Technology and Industry Scoreboard 2015: Innovation for growth and society*, OECD Publishing, Paris, http://dx.doi.org/10.1787/sti_scoreboard-2015-en. [28]

OECD (2012), *Machine-To-Machine Communications: Connecting Billions of Devices*, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2011)4/FINAL&docLanguage=En (accessed on 19 September 2017). [8]

OECD/ITF (2015), *Automated and Autonomous Driving: Regulation Under Uncertainty*, https://www.itf-oecd.org/sites/default/files/docs/15cpb_autonomousdriving.pdf (accessed on 21 September 2017). [44]

Ofcom (2017), *The Communications Market Report 2017: UK*, https://www.ofcom.org.uk/__data/assets/pdf_file/0017/105074/cmr-2017-uk.pdf (accessed on 19 September 2017). [26]

Popular Science (2017), *IBM could have a solution to one of self-driving cars' biggest problems | Popular Science*, 31 march 2017, https://www.popsci.com/ibm-self-driving-car-patent-prevent-crashes (accessed on 03 October 2017). [51]

Rivers, N. (2018), “Leveraging the Smart Grid: The Effect of Real-Time Information on Consumer Decisions”, *OECD Environment Working Papers*, No. 127, OECD Publishing, Paris, http://dx.doi.org/10.1787/6ad4d5e3-en. [36]

SAE (2014), *SAE International J3016 Standard*, https://www.sae.org/misc/pdfs/automated_driving.pdf (accessed on 21 September 2017). [45]

Sandvine (2016), *Global Internet Phenomena 2016 - Latin America & North America*, https://www.sandvine.com/downloads/general/global-internet-phenomena/2016/global-internet-phenomena-report-latin-america-and-north-america.pdf (accessed on 03 October 2017). [46]

Sebastian Soriano (2017), *The Internet of Things calls regulators to invent a pro-innovation approach – Medium*, Medium, https://medium.com/@sorianotech/the-internet-of-things-calls-regulators-to-invent-a-pro-innovation-approach-55a74147a7cb (accessed on 10 April 2018). [80]

Seeking Alpha (2017), *Verizon's (VZ) Management Presents at Goldman Sachs 26th Communacopia Conference (Transcript) | Seeking Alpha*, https://seekingalpha.com/article/4107060-verizons-vz-management-presents-goldman-sachs-26th-communacopia-conference-transcript?part=single (accessed on 10 October 2017). [69]

Semiconductor Engineering (2017), *Semiconductor Engineering .:. Prioritizing Vehicle Data Traffic*, 5 January 2017, http://semiengineering.com/prioritizing-vehicle-data-traffic/ (accessed on 03 October 2017). [49]

Seminconductor Engineering (2017), *Semiconductor Engineering:. Data Storage Issues Grow For Cars*, https://semiengineering.com/data-issues-grow-for-cars/ (accessed on 21 September 2017). [7]

Tech Crunch (2017), *Intel buys Mobileye in $15.3B deal, moves its automotive unit to Israel | TechCrunch*, 13 March 2017, https://techcrunch.com/2017/03/13/reports-intel-buying-mobileye-for-up-to-16b-to-expand-in-self-driving-tech/ (accessed on 03 October 2017). [52]

TechIn France (2018), *Règlement européen E-privacy Un coup d'arrêt à la transformation numérique ?*, http://www.techinfrance.fr/static/2018/02/12/e-privacy.pdf?AsnIo_Gg5tiX2OuyHtoSoA:jxSUTLVJsUe0iTkmebJeeA:LHczCbPxcBFBIbkN35dmDw (accessed on 10 April 2018). [79]

Telecom Italia (2017), *TIM: the Republic of San Marino is the first 5G State in Europe | Telecom Italia Group*, 17 July 2017, http://www.telecomitalia.com/tit/en/archivio/media/note-stampa/corporate/2017/TIM-Repubblica-San-Marino-MoU-5G-ENG.html (accessed on 06 October 2017). [62]

Telecom Lead (2017), *SK Telecom tests self-driving vehicle, plans to connect 5G later | TelecomLead*, 21 September 2017, http://www.telecomlead.com/5g/sk-telecom-tests-self-driving-vehicle-plans-connect-5g-later-79467 (accessed on 05 October 2017). [61]

TEVAC (2017), *Projet de Territoire d'Expérimentation Véhicule Autonome et Connecté*, https://pole-moveo.org/wp-content/uploads/2017/07/TEVAC-WP1-Executive-Summary_experimentations_vehicule-autonome-et-connecte_Vallee-de-la-Seine_%C2%A9Moveo_Imagine-Mobility.pdf (accessed on 10 April 2018). [43]

TNS and Bearing Point (2016), *Car manufacturers in the race for a connected future - BearingPoint*, https://www.bearingpoint.com/en/about-us/news-and-media/press-releases/car-manufacturers-in-the-race-for-a-connected-future/ (accessed on 22 September 2017). [32]

United States Department of Defense (2016), *DoD Policy Recommendations for The Internet of Things (IoT)*, https://www.hsdl.org/?abstract&did=799676 (accessed on 09 April 2018). [74]

United States Government Accountability Office (2017), *Internet of Things Status and implications of an increasingly connected world*, https://www.gao.gov/assets/690/684590.pdf (accessed on 09 April 2018). [76]

United States International Trade Commission (2017), “Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions”, https://www.usitc.gov/publications/332/pub4716_0.pdf (accessed on 09 April 2018). [73]

VB (2017), *Why Intel believes 5G wireless will make autonomous cars smarter | VentureBeat*, 20 May 2017, https://venturebeat.com/2017/05/20/why-intel-believes-5g-wireless-will-make-autonomous-cars-smarter/ (accessed on 05 October 2017). [57]

WEF (2015), *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services*, http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf (accessed on 09 April 2018). [78]

End Notes

[1] The United States Bureau of Economic Analysis of the United States Department of Commerce in 2018 publication on the measurement of the Digital Economy defined IoT as: "*Internet-enabled devices like appliances, machinery, and cars with embedded hardware allowing them to communicate with each other and connect to the Internet*" (Barefoot et al., 2018[1]).

[2] Namely, the BEA (2018) report mentions the following in page 9, "*BEA did not include structures and IoT infrastructure in the initial estimates because of the difficulty in determining the proper allocation of these categories into digital and non ‐ digital components. For both structures and IoT infrastructure, BEA does not have data available to separate digital economy activity from all other activity. The case of IoT infrastructure presents additional challenges. For example, the connectivity of an internet ‐ enabled refrigerator may allow the owner to track and purchase food items when they are running low or record usage of the appliance. However, the primary function of the refrigerator is to keep food cold, output which BEA would not classify as being part of the digital economy*" (Barefoot et al., 2018[1]).

[3] More examples of different uses and the most important network requirements can be found in Table 1 of the Ericsson report "5G Systems: enabling digital transformation" (Ericsson, 2017[2]).

[4] To name a few, the ITU had proposed a definition in 2012, the European Commission mentioned a definition a 2014 report, and the United States Department of Defence uses in its documents the IoT definition by the Institute of Electrical and Electronics Engineers (IEEE) (United States Department of Defense, 2016[7]).

[5] Namely, BEREC mentions the following in their previous work: *"IoT services are in varying phases of development and take various shapes, hence there is not yet a common understanding or definition of what IoT services and devices really are. […] For the purposes of this report, it is not necessary to determine in detail which definition is most appropriate.*" (BEREC, 2016[59])

[6] In April 2018, BEREC will conduct a survey to NRAs regarding IoT measurement, which will include questions trying to answer the following: What types of data measuring IoT are necessary and of most interest to NRAs? What definition(s) of IoT devices should be used? What is the best way to measure IoT network traffic?

[7] For example, if Volvo, a client of Telenor Connexion, sells an automobile with a SIM card, and this vehicle is sold outside Sweden anywhere around the world, it shows up in the M2M figures of Sweden provided by PTS. In this case, the Volvo vehicle shows up in the local network outside Sweden as a foreign roamer.

[8] In this sense, excluding certain objects that in other definitions are regarded as part of M2M will influence the indicator. In this regard, BEREC in its report on "Enabling the Internet of Things" (2016) mentions the following: "*Similarly, some stakeholders only regard such automated exchange between machines as M2M communication where no human beings are involved. However, according to other definitions, limited human intervention may be part of M2M communication. In this case, services which can be remotely controlled, such as via smartphones or tablets, may also be examples of IoT services, e.g. remote control of air conditioning and heating systems or the remote (un)locking of cars. However, this does not imply a general statement on the qualification of a service as IoT service with regard to all cases where an app on a smartphone or tablet is involved"* (BEREC, 2016[59]).

[9] They also use this definition in analysis trying to measure the total IoT market size. McKinsey in 2016 estimated that IoT market in 2015 represented up to USD 900 million, and would grow up to USD 3.7 billion in 2020, that is 32.6% CAGR. See McKinsey 2016 presentation *The Internet of Things: The IoT opportunity – Are you ready to capture a once-in-a lifetime value pool?* http://hk-iot-conference.gs1hk.org/2016/pdf/_04_Mc%20Kinsey%20-

%20(Chris%20Ip%20)%20ppt%20part%20%201%20_IoT%20-%20Capturing%20the%20Opportunity%20vF%20-%2021%20June%202016.1pptx.pdf

[10] According to the Ericsson Mobility Report 2017, Short Range IoT refers to the "*Segment that largely consists of devices connected by unlicensed radio technologies, with a typical range of up to 100 metres, such as Wi-Fi, Bluetooth and Zigbee. This category also includes devices connected over fixed-line local area networks and powerline technologies*".

[11] Please refer to the Ericsson Mobility Report 2017 in the section "The Internet of Things Outlook" (pg. 16), for more details: https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf

[12] In the 2016 Mobility Report, Ericsson would refer to these two IoT segments as Cellular and Non-Cellular IoT. The methodological change is that in the wide-range IoT segment in 2017, they now include both cellular IoT and Low-power technologies. See https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf . In addition, in the Mobility Report 2016, Ericsson estimated that IoT devices will grow from 15 billion devices in 2015 to 28 billion in 2021. In 2015 the composition of IoT was 0.4 billion Cellular IoT, 4.2 non-cellular IoT, 1.7 billion PC/laptop/tablet, 7.1 billion mobile phones, and 1.3 billion fixed phones. In 2021, most IoT connections will be Non-cellular IoT (14.2 billion).

[13] See the White Paper by the Ministry of Internal Affairs and Communications of Japan, Chapter 3, Section 3 (MIC, 2017[24]).

[14] The variety of household smart appliances is growing almost every day. In the United States, smart speakers are currently not mentioned in the households and individuals survey (NTIA, 2017[25]), despite their skyrocketing diffusion: according to a recent private survey, 16% of Americans aged 18+ owned a Smart Speaker at the end of 2017, and two third of them say that they wouldn't want to go back to life without their Smart Speaker (NPR, 2018[71]).

[15] Insurance companies start to provide a widening range of IoT "health related" devices to individuals (Le Monde, 2018[73]).

[16] The question used in the "CPS Computer and Internet Use Supplement", which is a survey block sponsored by NTIA and included the current population survey (IPUMS CPS, 2018[70]), is: "*What about interacting with household equipment or appliances that are connected to the Internet, such as a connected thermostat, light bulb, or security system? Do you use the Internet to interact with household equipment or appliances?*" (NTIA, 2017[25]).

[17] The definition of industrial robots used by IFR comes from the International Organisation for Standardisation (ISO) 8373:2012, which states that a robot is a machine with the following features: can be reprogrammed, is multipurpose in function, allows for physical alteration, and is mounted on an axis.

[18] The definition of "massive M2M communications" is analogous to the definition set forth by the ITU in their vision of the fifth generation of wireless networks, or the IMT 2020 standard, yet to be finalised in 2019 in the ITU's World Radio Communications Conference (ITU, 2015[82]). This standard is being conceived with IoT in mind with three main usage scenarios (i.e. enhanced mobile broadband, massive machine type communications, and critical communications/applications)

[19] In Ontario Canada, the rollout of smart meters to residential customers was completed by 2010 (Rivers, 2018[30]).

[20] Radar stands for Radio Detection and Ranging technology.

[21] LiDAR, Light Detection and Ranging, is a remote sensing method that uses light in the form of a pulsed laser to measure ranges.

[22] Another example of research projects in Europe involving automated vehicles is the case of French car manufacturers are currently working with the Institute VEDECOM (advanced research)

and the IRT System X (electronic architecture and cybersecurity) to run tests. While experiments on roads have been developed for many years in the United States, they only started in 2015 in France (CCFA, 2017[87]).

[23] See BEREC's report on "Enabling the Internet of Things", p. 4 (BEREC, 2016[46]).

[24] More examples of different uses and the most important network requirements can be found in Table 1 of the Ericsson report "5G Systems: enabling digital transformation" (Ericsson, 2017[2]).

[25] "*The latest agreements see Spain and Portugal signing a letter of intent to establish two joint corridors between Vigo and Porto, and Merida and Evora which will allow connected automated driving to be tested across borders. In addition, Italy and the three presidents of the Tyrol – Sudtirol – Trentino Euro region also confirmed their intention to work with other interested member states on the development of the 5G corridor on the Brenner Pass motorway*" (Mobile World Live, 2018[61]).

[26] A research project, linked with a French insurance company, is currently being conducted, on a platform implementation aiming at analysing the data flow originating from the connected objects, and focusing on protocols, density, type and modalities, and security measures linked to the data flows. Tests will include various specific markets (home smart devices, connected vehicles, wellbeing). Several object producers are involved, wishing to differentiate through a higher level of transparency on their products work and the respect of the user's privacy (Fondation MAIF, 2018[81]).

[27] An example of classification of data according to their usage purpose is provided by a case study on agriculture, where data are organised by the domain their relate to: agronomy –return of the cultures and quantity of input used-; machines –machines and equipment used-; and weather (TechIn France, 2018[80]).