Body of European Regulators for Electronic Communications

BEREC

BoR (18) 230

Draft

BEREC Public Consultation on Internet of Things Indicators

6 December, 2018

Contents

Introduction and objectives

BEREC has, in recent years and like many other organisations, started to consider the implications of the Internet of Things (IoT). In 2016, BEREC published a report on "Enabling the Internet of Things"[1].

In February 2017, BEREC held an expert "Workshop on the Internet of Things"[2], bringing together experts and stakeholders to discuss the regulatory implications and solutions required to "ensure a large-scale and sustainable IoT roll-out, in order to deliver significant benefits to citizens and consumers across different industries."

With this workshop, BEREC provided a forum for dialogue between National Regulatory Authorities (NRAs) and other competent authorities for matters regarding the IoT, as well as for other stakeholders in the industry, in order to create awareness and foster both an innovation-friendly and consumer-friendly environment.

Finally, with respect to the work of BEREC so far on the IoT, in March 2018, BEREC held an internal workshop on 5G and the IoT to outline the related security issues and discuss 5G implications on development of new services.

The current report, for public consultation, is prepared as a result of a project outlined in BEREC's Work Programme 2018[3], in which BEREC indicated that it would, in 2018, conduct an assessment on the type(s) of indicators that its constituent NRAs are collecting data for with regard to the IoT, as well as providing a more forward looking assessment with respect to what IoT indicators BEREC could look to collect data on, going forward, and why those indicators are important to BEREC.

Given the growth in the IoT, as evidenced by multiple studies and reports[4], and the consequential requirements for network resources, there is an ongoing and forward looking need for BEREC to reflect the importance of this sector in the work of BEREC. Depending on the outcome of the public consultation, BEREC could conduct further work, in future, to develop a harmonised set of indicators on the IoT for the purposes of benchmarking, and to provide a statistical overview of, the IoT landscape in Europe.

Much of the information presented in the subsequent chapters of the report is based on the results of two questionnaires which were circulated to, and answered by, experts of the NRAs. The questionnaires are set out in Annex 1 and Annex 2 of the report. In general, it covers the following topics:

- BEREC's IoT universe

[1] https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things
[2] https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/6972-summary-report-on-the-outcomes-of-the-workshop-on-iot-technologies-and-their-impact-on-regulation
[3] https://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/7528-berec-work-programme-2018
[4] For example, according to a 2015 study by European Commission, the number of IoT connections within the European Union (EU) is estimated to increase from approximately 2 million in 2013 to almost 6 billion in 2020.

- Effect of IoT on NRAs' spectrum policies and allocation of scarce resources
- The importance of IoT indicators for BEREC

In taking the results of those questionnaire, this report focuses on three of the four questions originally set out for this project in the BEREC Work Programme 2018, which were:

- What types of data measuring the Internet of Things are necessary and of most interest to National Regulatory Authorities?
- What definition(s) of Internet of Things devices should be used?[5]
- What is the best way to measure Internet of Things network traffic?

In light of expert discussion (among members of the BEREC Benchmarking Expert Working Group) ahead of the circulation of the questionnaire to NRAs, it was felt that it might be too early at this initial stage to achieve clear answers to the other question[6] originally set out for the project in the BEREC Work Programme 2018; i.e. the extent to which the European Commission's 2015 forecast has come to fruition – it is both too early and indeed, on reflection, not actually within the remit of this report to answer.

The overall objective of this BEREC report and public consultation, then, as set out in the BEREC Work Programme 2018, is to assess what, if any, are the indicators on the Internet of Things which NRAs are already collecting, primarily from the supply-side, but also on the demand-side, and to propose a way forward, if one exists, for any potential harmonised collection of IoT indicators by NRAs in order to benchmark and provide a statistical overview of the IoT landscape in Europe.

It should be noted that although many NRAs (depending on their national legislation) currently[7] don't/are not legally able to collect a lot of statistical information on the IoT, the responses to BEREC's recent questionnaires to NRAs suggest that there is a general agreement that some kind of broader monitoring (beyond M2M, for example) of the IoT should be targeted. In light of those NRA responses and the stakeholder responses to this public consultation, BEREC will look to address, and further consider, its position on the way forward. That way forward may, on the one hand, provide for a more high-level statistical information gathering process (covering, for example, the total number of IoT subscribers emanating from ECS undertakings and/or the quantity of national numbering resources allocated specifically to IoT), or it may, on the other hand, provide for a more granular statistical information gathering process (as further discussed on page 23 and elaborated in Figure 4).

BEREC has prepared this call for input with the aim of getting insights from all types of actors (consumers, companies in the telecommunications sector, digital companies, other companies, institutions) on issues to be taken into account by NRAs in the context of BEREC's approach to monitoring and collecting statistical information on the IoT. Specifically, BEREC

[5] Given that NRAs, in responding to the BEREC questionnaire, indicated a lack of definition for the IoT, generally, the report focuses less on devices and instead on the definition for the IoT more broadly.
[6] Establish to what extent the presented forecast in the Commission's 2015 study has come to fruition.
[7] The Electronic Communications Code will, once transposed, broaden the current powers to request data for all NRAs, Competent Authorities and BEREC.

is interested in the following issues that are addressed in the different sections of the public consultation:

1. **General issues regarding the collection of statistical information on the IoT, including a BEREC definition of the IoT.**
2. **BEREC's IoT universe, discussing the applications and network technologies that BEREC and NRAs should consider with respect to monitoring the IoT.**
3. **Effect of the IoT on NRA spectrum policies and scarce resources, covering the extent to which NRAs should monitor and BEREC should benchmark[8] IoT developments and the effects of such developments on spectrum and numbering requirements.**
4. **The importance of IoT indicators for BEREC, focusing on what NRAs currently collect and the potential future approach of BEREC in this area.**

Once BEREC has received all stakeholders' responses to this consultation, a report summarising their input will be published on the BEREC website. The contributions will be used in the preparation of the final report, expected to be completed and submitted for adoption at the BEREC Plenary meeting in March 2019.

[8] The overall ambition is that NRAs monitor the IoT and consolidate the information collected to create a benchmark of IoT across BEREC.

Instructions for submitting feedback to the public consultation

Once BEREC receives all responses, a report summarising that feedback will be published on the BEREC website[9] prior to the publication of the final version of the BEREC Report on Internet of Things Indicators, and the responses received will be used in the preparation of that report.

Timeline and subjective scope (target groups) of this public consultation

This consultation runs from 12 December 2018 to 23 January 2019. It is open to the wide range of public and private stakeholders involved in the IoT and to their associations. BEREC welcomes contributions from all stakeholders interested in the IoT, including:

- Public organisations at the local, national, and/or international level (e.g. competition authorities, government authorities, intergovernmental organizations, etc.);
- Industry: providers of ECNs (electronic communications networks and providers of ECSs), operators active along the IoT value chain – IoT services; players active along the value chains for data collection, data analysts; producers of smart handsets; and any other industry player active in the IoT sphere;
- Industry associations and networks;
- Consumers and consumers' associations; and
- Academia, think tanks, individual experts, individual citizens.

Instructions for submitting responses and transparency

This public consultation runs from 12 December 2018 to 23 January 2019. Please provide all answers to the questions in English. Respondents are not required to answer all sections and answers, although BEREC invites stakeholders etc. to submit contributions in as complete and detailed a manner as possible.

All non-confidential contributions to the consultation will be published on the BEREC website shortly after the end of the consultation period. Please, mention if any part or detail of your response has to be treated confidentially. Alternatively, you can provide a non-confidential version of your response.

[9] https://berec.europa.eu/

Responses should be addressed to pm@berec.europa.eu by close of business, i.e. 17.00 CET, on 23 January 2019. Responses received after this time and data will only be considered at BEREC's discretion.

Stakeholder information

Please provide the name (and website, if available) of your organisation, as well as the contact information (name, e-mail and/or phone number) for a contact person. In the case of personal contributions, please provide your name, nationality and contact information.

Name of the organisation/person, website, nationality and contact information

Please indicate the place(s) of operation of your organisation and the sector(s) in which your organisation mainly operates. Please explain how you are involved in the IoT.

Place(s) of operation, sector(s), and involvement in the IoT

1. General issues

In its 2016 report on "Enabling the Internet of Things", BEREC noted, when discussing terminology that "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." However, the report did reference a 2015 European Commission report[10], which defined the IoT as enabling "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 point being that in order to monitor and measure something, it must first be clearly set out as to what that something to be monitored and measured actually is. While BEREC could indeed use a definition for the IoT as elaborated by other organisations, and clearly it has already used the European Commission definition in the 2016 report, already mentioned, it would be worthwhile for BEREC to provide its own clear definition of what it considers the IoT to be; certainly with respect to the monitoring and measurement of the IoT.

This chapter provides some additional insight and information on various definitions for the IoT, which have been detailed by organisations and companies like the OECD (Organisation for Economic Cooperation and Development), the ITU (International Telecommunications Union), the GSMA (Global System for Mobile Communication Association), the IEEE (Institute of Electrical and Electronics Engineers), Gartner[11], and Vodafone. Additionally, information provided below is a review of some of the information that currently exists with respect to how the IoT is monitored and measured, i.e. what are the common indicators for the IoT.

Examples of definitions for the IoT

The OECD defines the 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 to be 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.[12]

In its 2012 paper, "Overview of the Internet of Things"[13], the ITU defines the IoT as 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. Through the exploitation of identification, data capture,

[10] "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination", Study prepared by IDC and TXT for the European Commission (2015): http://ec.europa.eu/digitalagenda/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination

[11] https://www.gartner.com/en; Gartner is a global research and advisory firm.

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

[13] Recommendation ITU-T Y.2060: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

For the GSMA, the IoT describes the coordination of multiple machines, devices and appliances connected to the Internet through multiple networks. Devices in the IoT cover many vertical industries; smartphones, tablets and consumer electronics, and others including vehicles, monitors and sensors equipped with M2M communications that allow them to send and receive data.[14] 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 IEEE has sought to focus on what they consider to be an ever-changing definition of the IoT. In 2015, the IEEE released a paper[15] intended to establish a baseline definition of the Internet of Things, in the context of applications that range from small, localised systems to larger global systems, geographically distributed and composed of smaller localised systems. Given this, the IEEE defines the smaller system as follows:

> *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.*

The IEEE's definition of the larger system is essentially then the interconnection of a large amount of 'Things' in order to deliver a complex service and support an execution of complex processes.

Gartner defines the IoT as the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.[16] Indeed, Cisco in its recent research on the IoT [17] utilises the Gartner definition for its purposes.

Finally, in terms of the variety of definitions available for the IoT, Vodafone, in its annual "IoT Barometer"[18], defines the IoT as connecting objects, turning them into intelligent assets that can communicate with people, applications and each other. The IoT enables things like cars, buildings and machines to communicate about their status and environment.

It is clear from this shortlist of definitions that there are sufficient commonalities to allow for BEREC to assess and define its own clear and agreed description of the IoT, which will aid any future harmonised gathering of data for indicators on the IoT. However, given the previous use of the European Commission's definition, unless BEREC considers it necessary to have its own definition, the Commission's wording should be sufficient in the short term for any work that BEREC conducts regarding the IoT.

---

[14] https://www.gsma.com/iot/wp-content/uploads/2016/09/What-is-the-Internet-of-Things.pdf
[15] "Towards a definition of the Internet of Things (IoT)", IEEE (2015): https://iot.ieee.org/definition.html
[16] https://www.gartner.com/it-glossary/internet-of-things/
[17] https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf
[18] https://www.vodafone.com/business/news-and-insights/white-paper/iotbarometer

Examples of monitoring and measurement of the IoT

Before assessing the statistical information that NRAs collect in this field, it is worthwhile to provide an overview of the type of monitoring and measurement being conducted elsewhere. Given the general theme that finding reliable data about the installed base of IoT devices, market size and valuation is currently not easy.

However, typically available (whether freely or in commercial market reports) information based on forecasts and/or surveys can provide a useful benchmark, particularly when the point is reached whereby NRAs can actually collect statistical information on a harmonised set of indicators for the IoT.

This might, indeed, allow for an assessment of the veracity of the forecast presented by the European Commission, which was mentioned in the original outline for this project.

Some examples of information on the IoT available freely or in commercial market reports include:

- Gartner Forecast - Internet of Things[19]: Gartner forecasted that 8.4 billion connected things would be used worldwide in 2017, up 31% from 2016, and will reach 20.4 billion by 2020.
- Cisco Visual Networking Index[20]: According to Cisco, 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.
- Cisco Cloud Index White Paper[21]: Globally, the data created by Internet of Everything devices will reach 507.5 ZB per year (42.3 ZB per month) by 2019, up from 134.5 ZB per year (11.2 ZB per month) in 2014. Globally, the data created by Internet of Everything devices will be 269 times higher than the amount of data being transmitted to data centres from end-user devices and 49 times higher than total data centre traffic by 2019.
- IDC Worldwide Internet of Things Forecast[22]: By 2021, global IoT spending is expected to total nearly €1 trillion as organizations continue to invest in the hardware, software, services, and connectivity that enable the IoT.

[19] https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016
[20] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visualnetworking-index-vni/mobile-white-paper-c11-520862.pdf
[21] http://cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html
[22] https://www.idc.com/getdoc.jsp?containerId=prUS42799917

- IHS Enabling the Internet of Things[23]: Forecast of global IoT installed base from 2015 to 2025.

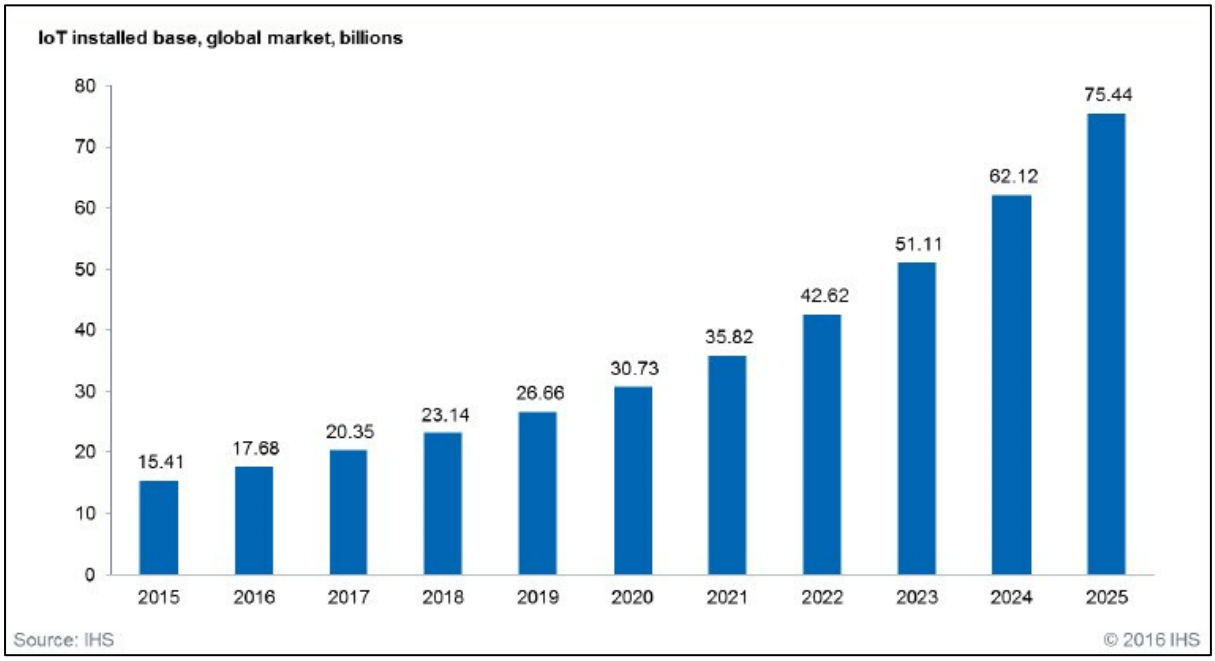


Figure 1: IoT installed base. Source: IHS.

One final example of how statistical information is used to monitor and measure the IoT is Vodafone's annually published IoT Barometer[24]. In the 2017/2018 edition, Vodafone interviewed almost 1,300 business respondents globally, and covered multiple industries and company sizes. According to its analysis, Vodafone states that IoT adoption has grown from 12% of respondents to their survey in 2013 to almost 30% in 2017. Further, according to Vodafone, many respondents have increased their number of connected devices. Finally, based on Vodafone's survey, the proportion of companies embracing the IoT "on a massive scale" – over 50,000 connected devices – has doubled since 2016.

Stakeholder questions

Question 1.1:

Do you consider that the European Commission's definition of the IoT is sufficiently appropriate to collect relevant statistical information on the IoT? If not, how should the definition be changed?

Answer to question 1.1:

[23] https://www.ihs.com/Info/0416/internet-of-things.html
[24] https://business.vodafone.com/barometer2017#download

Question 1.2:

Please suggest any available sources for information on measures/indicators of the IoT, in addition to the information mentioned above.

Answer to question 1.2:

2. BEREC's Internet of Things universe

With respect to existing definitions for the IoT, the landscape is very broad and there are many different viewpoints from which IoT can be distinguished. The different definitions may overlap with each other or have some specific aspects which differentiate. Thus, the specific distinction of IoT depends on individual perspectives, which leads, overall, to relatively vague understandings of the term 'Internet of Things'. As a starting point for profiling the BEREC 'Internet of Things universe', a broad definition may be appropriate to begin with, followed by case-specific determinations.

Boundaries to the IoT

According to ITU-T Y.2060[25], the IoT is 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. A thing with regard to the IoT is an object of the physical world (physical thing) of the information world (virtual thing), which is capable of being identified and integrated into communication networks.

Through the exploitation of identification, data, capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled. From a broader perspective, the IoT can be perceived as a vision with technological and societal implications."

From a regulatory perspective, in the past, the focus was on services eventually foreseen for the use of IoT/M2M. In particular, the focus was on the number of SIM cards used for M2M-transmission services. The background of this restriction lies within the regulatory framework, which allowed NRAs only to oversee telecommunication markets and the respective providers of electronic communication services.

This situation only covers parts of the markets for IoT and does not allow a complete assessment of the markets and the evolution of IoT. The future regulatory framework, namely the European Electronic Communications Code (EECC)[26], would allow NRAs to also consider adjacent markets. Thus, in future, NRAs will be able to generate a more comprehensive assessment of the IoT.

In addition to new competences from the EECC, it may, however, still be impossible to gather a complete overview on IoT markets, since the IoT can be used via private communication networks; for example, a company-wide WiFi-network, or private Bluetooth- or ZigBee[27]-based network. The following illustration gives an initial, broad overview of the boundaries of the IoT. Further detail on this broad overview is elaborated on and itemised later in this document, with a focus on the IoT which is not based on private/non-commercial networks.

[25] "Overview of the Internet of Things; https://www.itu.int/rec/T-REC-Y.2060-201206-I
[26] https://www.consilium.europa.eu/en/policies/electronic-communications-code/
[27] https://www.zigbee.org/what-is-zigbee/

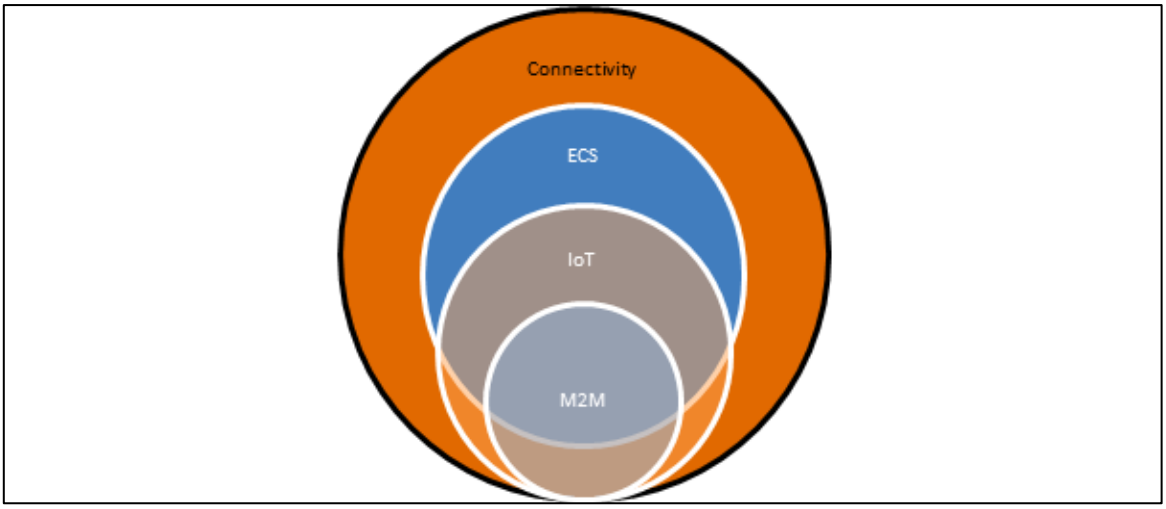


Figure 2: the boundaries of the Internet of Things. Source: BEREC.

- **Connectivity**
  - Every IoT/M2M-service depends on some form of connectivity, for example, via:
    - Traditional electronic communication service (ECS)
    - Commercial networks in unlicensed spectrum (for example, SigFox, TheThingsNetwork[28]) or private networks (for example, WiFi, Bluetooth, ZigBee).
- **ECS**
  - This comprises traditional ECS, for example, ISDN/SMS/data[29], including:
    - Dedicated M2M-transmission services, for example, M2M-services offered by a provider of mobile communication services
    - Internet Access Services.
- **Internet of Things**
  - Comprises the applications of IoT
  - Connectivity via ECS provided through public or private networks.
- **M2M**
  - In BEREC's 2010 report on convergent services[30] M2M is described as "a generic concept that indicates the exchange of information in data format

[28] https://www.thethingsnetwork.org/
[29] Given that M2M communication is based on data transmission.
[30] https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/210-berec-report-on-convergent-services

between two remote machines, through a mobile or fixed network, without human intervention."

- M2M is a subset of the IoT, and is the combination of ICT and smart, connected devices that allows such devices to interact without any human intervention.

Broadly speaking (beyond the specific context of this document) what is meant by "human intervention" remains to be explicitly defined; beginning with "no human intervention" via "little human intervention" to "limited human intervention". M2M communication may also be offered through a mix of proprietary and standardised technologies and, to this effect, the M2M definition above merits some amendments to make it technology neutral by removing specific references to mobile and fixed networks. Moreover, the notion "M2M communication" is used in order to describe the (technical) connection between an IoT device and a data centre, between two devices or the like, which is underlying an IoT service.[31]

NRAs' considerations on BEREC's IoT universe

In its supplementary questionnaire on IoT indicators, BEREC provided NRAs an initial draft illustration (see Annex 2 of this document) of what could be considered in BEREC's universe. Some of the key responses received include the following:

- Distinguish between data-heavy/capacity-heavy and non-data/capacity-heavy IoT devices/services (e.g. devices sending short text strings on a minimal scale such as water level sensors versus data heavy services such as video with continuous streams or services requiring high latency such as medical applications).
- Better to form a more general view of the development of the IoT rather than seek to grasp every detail.
- Taking into account RSPG17-006 "A Spectrum Roadmap for IoT"[32], professional mobile radio networks (PMR) could be added, as well as point-to-point and point-to-multipoint systems, and satellite networks.

Illustration of BEREC's IoT universe

In the broad overview set out above, the IoT "set" is vague and could include many different services, applications and devices. To be able to assess the markets of IoT, there is a need to focus on some (of the most important) IoT applications and underlying network

[31] https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things

[32] https://circabc.europa.eu/sd/a/a0faa1a5-ca41-42c3-83d5-561b197419b0/RSPG17-006-Final_IoT_Opinion.pdf

technologies. As a first suggestion, those most important categories could be the industrial sector, the automotive sector and the consumer sector.[33]

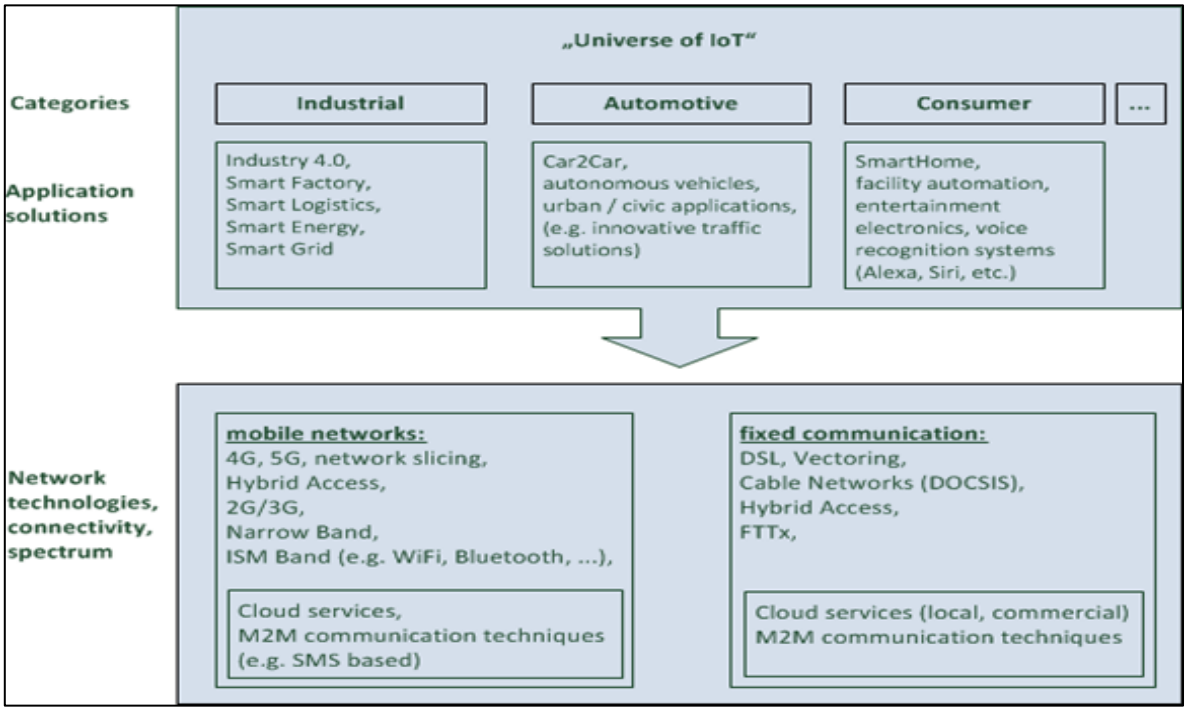


Figure 3: BEREC's proposed IoT universe. Source: BEREC.

- *Industrial Internet of Things (IIoT)*

The IIoT can greatly improve connectivity, efficiency, scalability, time savings, and cost savings for industrial organisations. Companies are already benefitting from the IIoT through cost savings due to predictive maintenance, improved safety, and other operational efficiencies. However, interoperability and security are probably the two biggest challenges surrounding the implementation of IIoT. A major concern surrounding the Industrial IoT is interoperability between devices and machines that use different protocols and have different architectures.

- *Automotive Internet of Things (AIoT)*

There exist several use cases in the automotive sector which are based on communication between vehicles. Mainly they should improve road safety and prevent accidents. For example, a car could inform another vehicle that is approaching about a potential danger. In addition autonomous cars can help to make the use of the existing infrastructure more efficient and could also increase the comfort of the users, who can make other use of their travel time. These developments, which are currently in progress in the automotive sector require a comprehensive connectivity of the vehicles.

[33] It should be noted that a small cohort of NRAs indicated in their responses to BEREC's IoT questionnaires that collecting IoT indicators at the granularity of service/application level would be very taxing for service providers.

- *Consumer Internet of Things (CIoT)*

In essence, CIoT refers to the IoT in the context of consumer applications, use cases and devices (for example, wearables). “The whole idea of CIoT is to continually gain consumer insights and implement the same in creating customised products and services.”[34]

Stakeholder questions

Question 2.1:

Do you agree with the multi-layered approach in Figure 2 above, which seeks to separate M2M/IoT from the underlying connectivity and shows the relationship to ECS?

Answer to question 2.1:

Question 2.2:

What is your opinion on the differentiation of IoT and M2M? Do you have any additional proposals regarding such differentiation?

Answer to question 2.2:

Question 2.3:

In relation to application solutions, do you see the three categories “Industrial”, “Automotive” and “Consumer” as the most relevant? Would you suggest other categories? If so, please elaborate.

Answer to question 2.3:

[34] https://medium.com/@sahana_63956/introducing-consumer-internet-of-things-ciot-and-its-evolution-d6e2785cb3cb

3. Effect of the IoT on NRAs' spectrum policies and allocation of scarce resources

The IoT is a hugely important and rapidly growing market. The connectivity revolution powered by M2M and the emerging IoT is one of the most important trends in modern technology and is set to transform countless industries. Mobile services play an important role in the wide area M2M and IoT markets. According to the GSMA[35], the bulk of the M2M market uses short-range, unlicensed connections (e.g. WiFi, ZigBee etc.), however the wide area market is heavily reliant on mobile connectivity. Furthermore, as forecasts indicate that the number of IoT connected devices worldwide is set to rise dramatically and reach 26 billion by 2020, the need for IoT devices to be identifiable in the network will persist, as it does today for traditional voice and data devices, although IoT devices are fundamentally different from traditional devices.

However, many of the requirements associated with the use of E.164 (the traditional telephone numbers) ranges are inappropriate for the large majority of IoT connected services. Requirements related to current numbering regulation such as number portability are not relevant with respect to the IoT, as the service does not directly involve an individual and the connectivity element is just an enabler of the entire service wrap. Given that the majority of BEREC NRAs have both spectrum and numbering responsibilities, BEREC considers it important to consider these aspects with respect to any potential future monitoring of the IoT. Therefore, the following sections cover the responses to questions in the supplementary questionnaire on these matters.

IoT and NRA spectrum policies

The spectrum needs of IoT applications are determined by their throughput requirements, but also coverage, latency and reliability. For a given spectral efficiency (b/s/Hz), the lower the latency requirements the larger the bandwidth needed to send a given amount of data - this becomes very important for applications such as remote surgery. E-health applications often need ultra-reliable connections (security and privacy), and the combination of ultra-robust connections (heavy coding and retransmissions) with high throughput/low latency requirements requires large bandwidths. Spectrum bands suitable for IoT are determined by each IoT application's range and coverage requirements as well as bandwidth needs of the applications. Range and coverage requirements also depend on deployment scenarios.

A number of NRAs indicated, in their response to the specific question as to what effects on spectrum policy do they expect the development of the IoT to have, that monitoring of spectrum management developments already takes place at an EU level with organisations other than BEREC (for example, CEPT, ETSI, ITU-R). However, while there may not be a necessity to launch a monitoring of technical issues of spectrum usage within BEREC, as this may overlap with these other organisations' work, best-practice sharing among NRAs could

[35] https://www.gsma.com/spectrum/wp-content/uploads/2017/05/Spectrum-IOT-Position-Paper.pdf

be useful, especially in the case of future 5G-based M2M services, in order to find the best opportunities or solutions for the introduction of 5G.

Some NRAs pointed out that the development of the IoT could have consequences in terms of spectrum policy, for example:

- The allocation of appropriate frequency bands for IoT, either licensed (LTE-M, NB-IoT) or license exempt,
- The adaptation of the technical conditions of use of the frequency bands, to reflect the technological evolutions of IoT.

Regarding the first point above, the bulk of the M2M market uses short-range, unlicensed connections (for example, WiFi, ZigBee etc.). The wide area market is heavily reliant on mobile connectivity; there exist high quality of service guarantees over wide areas, as operators are not at risk of interference and can control usage levels. There is, therefore, a whole portfolio of different use cases and a whole range of different needs for different type of IoTs. In terms of spectrum requirements, provisions have to be made within both the licence exempt frequency band and also within the licensed frequency band.

Monitoring the development of IoT would help the NRAs to adjust their spectrum policy accordingly. One NRA indicated that it has already started the forward-looking process by identifying spectrum ranges suitable for narrowband, wideband, short or long-range IoT applications. Frequency options for IoT applications include public or private mobile networks as well as license exempt frequencies for short range devices. These frequency options enable a very flexible and adaptable environment for IoT applications to address their specific demand. It is expected that IoT applications are an essential driver for the implementation of 5G including network slicing within the limits of identified spectrum for public mobile operators. Monitoring the specific spectrum use of IoT applications may therefore be essentially to define future demands. Furthermore, for capacity planning, it is important to know the estimated amount of data traffic based on technologies where regulation is in place (in particular cellular/mobile technologies or other types of licensed spectrum).

IoT and NRA allocation of scarce resources

In its supplementary questionnaire to NRAs, BEREC asked the following questions:

- With regard to the expected growth in the use of IoT devices, do you see the necessity for NRAs/BEREC to monitor these developments?
- Do you see the need to monitor which national numbers for IoT devices are used outside your territory (and vice-versa, which numbers assigned in other countries are used in your territory)?

Regarding the first question, in terms of the necessity to monitor the expected growth in the use of the IoT, the response by NRAs was unanimous, in that all indicated a need to monitor these developments. One NRA noted that the expected proliferation of IoT devices may lead

to a high demand for national numbering and network resources, hence it is important for national NRAs to monitor developments in the IoT market.

Since numbers are a scarce resource and the use of IoT devices could increase dramatically in the coming years, monitoring these developments is important to identify expected demands as early as possible. NRAs will need to monitor the increased demand of numbering, prepare national plans accordingly and monitor the development of needs in this area.

Regarding the second question, some NRAs indicated the need for more evidence (i.e. the size of such markets) to assess this matter. Reasons pointed out by some NRAs against the necessity to monitor extraterritorial use of national numbers for IoT devices are that numbering rules apply for these numbers are the same whether they are assigned to users domestically or abroad. Reasons in favour of this monitoring indicated are that this information (i.e. information gleaned from monitoring which national numbers for IoT devices are used outside of a specific country's territory) would be helpful in order to keep an overview of the geographic distribution of the resources.

In addition, such information would be useful with respect to M2M/IoT roaming, which would have implications for potential security issues nationally, in the EU and beyond. It should also be noted that in light of the new EECC, BEREC has been tasked with developing a database of numbering resources with a right of extraterritorial use within the EU. This database could be sufficient to achieve such monitoring. BEREC also asked NRAs as to the relevance of these matters (i.e. monitoring of expected growth of IoT and of extraterritorial numbers) for NRAs and/or for other national authorities. Responses to this question typically noted that while, for the former question, it is of utmost relevance to NRAs, for the latter it is of most relevance to authorities responsible for public security and criminal enforcement/IT security. However, it can also be considered relevant for NRAs for the purposes of statistical analysis, interpretation, and the operation of security-related information tasks.

Based on the elaboration of the boundaries of the IoT, set out above in Figures 2 and 3, some elements of the IoT market may well be considered outside of the scope of classical/current telecoms regulation, which has its roots in the opening of the formerly monopolised/state owned telecoms markets characterised by very high investment cost and high barriers to replication of infrastructure. Historically, the regulation was set up to create competition and to assure that each end-user had access to basic telecom services at affordable cost and at sufficient quality. As long as IoT does not create totally new end-user activities, but "only" refines/automates existing activities (car travel, heating/ventilation/lighting of buildings, medical appliances, assurance of public security, etc.) the existing authorities have to adapt to and deal with IoT in their respective field of activities.

Stakeholder questions

Question 3.1:

In your opinion, what effects on spectrum policy is the development of the IoT expected to have, and do you think it's necessary for NRAs to monitor, and BEREC to benchmark, these developments?

Answer to question 3.1:

Question 3.2:

With regard to the expected growth in the use of IoT devices, do you see the necessity for NRAs to monitor, and BEREC to benchmark, these developments, particularly with respect to numbering? If so, why?

Answer to question 3.2:

Question 3.3:

Do you see the need for NRAs to monitor which national numbers for IoT devices are used outside their domestic market/territory (and vice-versa, which numbers assigned in other countries are used in the NRA's territory)? If so, please elaborate.

Answer to question 3.3:

Question 3.4:

In your opinion, in addition to NRAs, for which entities (EU and non-EU) are the following individual matters relevant:

(a) The effect of IoT on spectrum policy

(b) The effect of IoT on scarce resources, i.e. numbering

(c) The monitoring of national numbers for IoT devices used on an extraterritorial basis

Answer to question 3.4:

4. The importance of IoT indicators for BEREC

Between July-October 2018, NRAs submitted information, in response to two questionnaires on the IoT, to BEREC. These questionnaires focused on the current data collection processes of NRAs with respect to the IoT[36] as well as on why the IoT is of importance to BEREC[37], particularly on what type of indicators BEREC should look to collect data on going forward. The two sections below present information, at a high level, on the responses to those questionnaires, with particular emphasis on why NRAs consider such a focus on IoT indicators to be important for BEREC.

Current NRA approaches to collection of IoT statistical information

According to their responses to BEREC's questionnaire on current data collection processes with respect to the IoT, most NRAs indicated that they do collect some statistical information on the supply side (i.e., from operators/service providers). However, statistical information collected is almost exclusively related to machine-to-machine (M2M). While one NRA began collecting data on M2M as far back as 2000, typically, the regular collection of statistical information of this type started in 2010, with some NRAs particularly being at the vanguard of such collection. In general, the M2M-related statistics that are collected by NRAs include the number of subscriptions, data volumes and revenues. In addition, some NRAs elaborated on statistical information on the IoT sourced from the demand side (i.e. from consumer or business surveys) but, again, this was limited to M2M type data.[38]

In responding to BEREC's first questionnaire (see Annex 1) only a small cohort of NRAs indicated that they would collect statistical information on the IoT beyond that which is already being collected (i.e., as set out above, statistical information on M2M) in the short to medium term, i.e. during the next 12-24 months, before the deadline for transposition of the new Code. NRAs weren't asked to comment on the longer term and their collection of such statistical information. The other responses received were either clearly negative (as in the NRA has no plans in the short-run to collect such information), or that there was uncertainty as to whether such a future collection of statistical information would take place. At the same time, when responding to a question regarding the need for BEREC to benchmark the IoT, a significant number of responding NRAs (more than 10) agreed that there is such a need.

Given that the collection of statistical indicators on the IoT currently focuses on rather general information on M2M, some of the responding NRAs suggested that a step forward would be to just expand the M2M statistics that are collected. This could potentially be achieved by collecting additional data on the specific sectors the M2M services are used within (for example, industry, health, automotive, agricultural etc.). By keeping this information at the

[36] Questionnaire presented in Annex 1.
[37] Questionnaire presented in Annex 2.
[38] For example, UKE (the Polish NRA) indicated that in a 2017 consumer survey 23% of respondents had heard about the Internet of things (Machine to Machine); 11% of respondents used M2M SIM cards; 9% of respondents were thinking about usage of connected devices. Typically, respondents used connected devices in the home (73%), while 26% used such connected devices in the workplace. The respondents that used services IoT/M2M services generally used SMS bundles (24%).

sectoral level only, it would not include significant 'sensitive' information. However, it should be noted that M2M data presents a very narrow and perhaps random view of the development of the IoT.[39]

Most NRAs have, under current legislation, mainly the right to gather indicators from service providers in the field of electronic communications. Given the new EECC[40], it may be possible to gather data from adjacent sectors to the telecommunications sector. This could open up the possibilities to gather more useful indicators of IoT, beyond the current data covering M2M. The usefulness of such indicators of IoT should be reflected in requests for information, which should, in turn, be proportionate and sufficiently reasoned. In light of this, NRAs also provided responses to a more forward looking questionnaire circulated by BEREC, the responses to which are synthesized in the following section.

Suggested areas for BEREC approach to IoT statistical information

In responding to BEREC's supplementary questionnaire on the IoT, several NRAs elaborated on their reasons for, and provided clarity on the benefit of, a BEREC common approach regarding the IoT. Such possible benefits of a BEREC common approach regarding statistical information on the IoT include:

- A global BEREC approach would be an asset at two levels:
    - guide EU Member States in their choices related to players to question and data to collect,
    - in having a harmonized approach regarding IoT market at a European level.
- Common approach to benchmarking of IoT indicators could be considered useful for harmonisation of data collection and for sharing experiences/best-practices among NRAs. This could help to make the IoT market more transparent and also could contribute to the development of IoT environment, especially in context of deploying 5G networks in EU.
- A common approach with respect to IoT data collection and benchmarking may prove beneficial since they can be compared on a 'like with like' basis across all member states. However, any IoT data requests should be kept as high level as possible.
- In general, it would be of benefit to achieve a common understanding of IoT in all EU Member States. Since IoT products presumably are used EU-wide or even world-wide, the evaluation of the development of the usage and distribution of IoT devices should

[39] The NRA that provided such commentary noted that it was not certain as to whether the current indicators (i.e. M2M subscriptions etc.) can provide a very reliable benchmark. It's possible that consumer surveys might provide more complete insight but only for household use.

[40] The EECC makes reference to situations where information requests to undertakings are insufficient for national regulatory authorities – in such situations, in order for other competent authorities and BEREC to carry out their regulatory tasks under EU law, such information may be requested from "other relevant undertakings" active in the electronic communications or closely related sectors

be implemented at least on EU level. Further to compare IoT markets in relation to traditional ECS-markets, an EU benchmarking would be helpful for providers which are operating in more than one member state.

At the same time, some NRAs responded with some uncertainty on the importance for BEREC to have a common approach with respect to the IoT data collection. In particular, these uncertainties steam from the fact IoT have been outside of the typical competencies of telecoms regulators and, thus, the concrete purpose of collecting IoT indicators needs to be clearly defined (in particular, for those NRAs that would collect these data for the first time). Any data request might have to be kept as high level as possible, at least in the short/medium term. One of BEREC's main tasks is to improve the consistency of the application of European telecom rules, and contribute to the development of the Digital Single Market and the European Gigabit Society.[41]

Given the possibilities under the new EECC, it would be beneficial to achieve a common understanding of the IoT in all EU Member States. There are, of course, other types of benefits with respect to such harmonisation, for example, common terminology, comparable data, and tracing transnational use of the IoT.

While it is difficult to identify and determine common indicators prior to knowing the extent which the regulation will actually affect the possibilities, this section identifies some suggested potential areas in which it would be beneficial to collect data, if the regulation allowed it. Figure 4 below graphically illustrates the general areas of IoT indicators proposed by multiple NRAs to BEREC, in response to its supplementary questionnaire on the matter.

One suggested area of indicators includes the types of network used for the IoT devices to communicate. Furthermore, several responses suggested that the number of devices, including types of users, are interesting to collect (for example, industrial use or residential devices) as well as which sectors or domains the devices are used in.

While capacity is pivotal for the network, IoT devices affect the network in several ways depending on the type of device. Hence, the total number of IoT devices alone is of less importance if the network impact is not included. This would add a competition perspective and identify how IoT devices strains the potential bottlenecks within the network.

In addition there are other types of volume data that could be interesting to collect beyond the scope of network capacity. Another relevant area for statistical indicators could be prices and price-models for the different IoT networks and services.

[41] https://ec.europa.eu/digital-single-market/en/policies/improving-connectivity-and-access

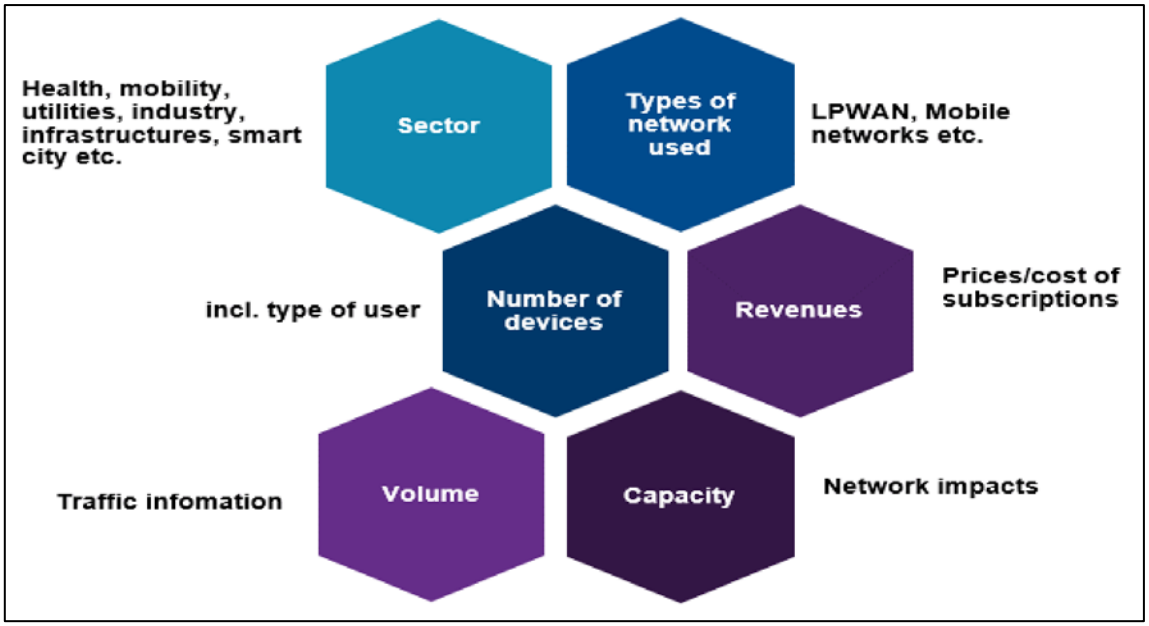


Figure 4: General areas of interest for future indicators according to NRAs. Source: BEREC.

According to NRAs, revenues are important for an assessment of the relevance of IoT markets in relation to traditional ECS-markets. Statistics on the number of users (broken down by usage) and the traffic generated are important to develop an understanding concerning the domains of IoT, and needed with respect to providing evidence in regulatory decisions made by NRAs. Statistical information relating to capacity could inform NRAs about connectivity needs.

The statistical indicators proposed for future collection are similar in nature to the suggested way forward with respect to the current M2M data that is collected. However, NRA responses suggest that, in time, there will exist a need for indicators on also machine-to-person (M2P) and person-to-person (P2P). P2P connections are characterized by collaborative solutions that leverage new and existing network infrastructure, devices, and applications. M2P connections mean that people can send information to technical systems and receive information from these systems (for example, receive data and analytics). All of these connections are transactional, which means the flow of information moves in both directions, from machines to people, from people to machines or from machines to other machines. However, it is unclear if such indicators would fall under the current remit of NRAs.

Overall, NRAs suggested that BEREC needs to gather such IoT-related statistical information for some of the following reasons:

- IoT is an emerging market with far reaching possibilities
- Interesting to learn what kind of value added layer emerges and to what extent MNOs try to cover all demand on their own
- Give a correct picture of the mobile markets (not to hide IoT in global SIM card data), to be able to calculate market shares and describe markets in a more detailed fashion
- Understand as to whether IoT could develop towards a European market, or if it (and to what extent) remains a national market

- Add to a basic set of information concerning data economy issues
- Progress towards data-based regulation, opening such data (after anonymisation when required) to external entities
- Having reliable, market-based knowledge is central to the strategy of NRAs.

Stakeholder questions

Question 4.1:

What is your opinion on the benefit of a BEREC common approach regarding the IoT?

Answer to question 4.1:

Question 4.2:

Do you agree with the general areas of interest for future indicators (to be collected), presented in Figure 4 above? Could you suggest any specific IoT indicators that BEREC should consider for collection?

Answer to question 4.2:

Question 4.3:

Do you support the gathering of statistical information on IoT by BEREC? Please substantiate your answer.

Answer to question 4.3:

5. Other issues

This section covers any other issues relating to IoT indicators that have not been addressed in previous sections/questions, and which stakeholders consider to be of potential interest to BEREC in the context of the report to be prepared subsequent to the Public Consultation.

Stakeholder questions

Question 5.1:

Are there any additional issues relating to collection of statistical information on the IoT which have not been included in previous questions that you would like to address?

Answer to question 5.1:

Annex 1: Questionnaire on IoT indicators

Benchmarking Expert Working Group
BEREC questionnaire to inform a report for consultation on a set of indicators to measure the Internet of Things

Q#	A) Collection of statistical information on the Internet of Things	
1.	Does your NRA collect any statistical information on the Internet of Things? Any statistical information could be data on the Internet of Things in the broadest sense (see definitions) or any subset of the Internet of Things such as M2M SIM cards or traffic, number of connected devices, Internet of Things applications, etc. (Please provide your **Yes / No / Don't know** answer **in the box to the right.**) ***If you answered Yes to Q1 please proceed to Q2, and continue to answer the rest of the questions where possible.*** ***If you answeied No or Don't know to Q1 please proceed to Q10, and continue to answer the remaining questions where possible.***	
2.	Is this statistical information collected from the supply-side, i.e. questionnaires to operators or vendors? (Please provide your **Yes / No / Don't know** answer **in the box to the right.**)	
2i.	If you answered Yes to Q2, please provide a link or some detail of the questionnaire to collect such statistical information **in the box below.**	
3.	Is this statistical information collected from the demand-side, i.e. consumer or business surveys? (Please provide your **Yes / No / Don't know** answer **in the box to the right.**)	
3i.	If you answered Yes to Q3, please provide a link or some detail of the survey to collect such statistical information **in the box below.**	
4.	Does your NRA have its own definition of the Internet of Things, in terms of how the technology is defined when asking questions of operators/vendors and/or asking questions of consumers/businesses with respect to the collection of statistical information on the Internet of Things? (Please provide your **Yes / No / Don't know** answer **in the box to the right.**)	
4i.	If you answered Yes to Q4, please provide details of the definition, and how the NRA came to this definition, **in the box below.**	
4ii.	If you answered No to Q4, please provide details of the definition of the Internet of Things that your NRA uses, **in the box below.**	

B) Details of indicators and NRA experience in the collection of statistical information on the Internet of Things

5. If your NRA collects supply-side or demand-side statistical information on the Internet of Things, can you provide some detail (**in the table to the right**) on the types of service (for example - healthcare, connected cars, wearable devices, household equipment) and the indicators (for example - subscriptions, usage (data volumes), revenues) per service that your NRA collects statistical information on? Where relevant, in the Notes column, please include any information on the types of surveyed operators (for example - IoT LPWAN operators, IoT service providers, Mobile Virtual Network Operators etc.)

Type of service	Type of indicator	Type of collection (supply-side, demand-side)	Sources of information (i.e. responses to operator/vendor questionnaire or consumer/business survey)	Notes

6.	How is the information on Internet of Things services used by your NRA, i.e. what is the objective of / reason for collecting this information? Please provide details **in the box below.**	
7.	When did your NRA start collecting such information, and how often is it collected (quarterly / semi-annually / annually)? Please provide details **in the box below.**	
8.	What is your NRA's experience in researching or collecting statistical information on Internet of Things services, i.e. what have been the main difficulties? Please provide details **in the box below.**	
9.	Is there a legal basis (in national legislation) that allows your NRA to request and obtain this information from telecom operators and/or other sources? (Please provide your **Yes / No / Don't know** answer **in the box to the right.**)	
9i.	If you answered Yes to Q9, please provide details **in the box below.**	

C) Forward looking opinion and broader market experience of collection of statistical information on the Internet of Things

10.	Is your NRA planning to ask (either on the supply-side or demand-side) for statistical information on any Internet of Things indicators during the next 12-24 months? **(Yes / No / Don't know)**	
10i.	If you answered yes to Q10, please provide details of what indicators your NRA will seek to collect **in the box below.**	
11.	In your NRA's opinion, is there a need for a benchmarking of Internet of Things indicators (to compare adoption of Internet of Things connected devices across European countries) by the European Commission or BEREC within the next 12-24 months? (Please provide your **Yes / No / Don't know** answer **in the box to the right.**)	
11i.	If you answered Yes to Q10, please provide details **in the box below.**	
12.	Is your NRA aware of the existence of statistical information on Internet of Things services collected and/or published by other organisations in your Member State, or more broadly across the EU? (Please provide your **Yes / No / Don't know** answer **in the box to the right.**)	
12i.	If you answered Yes to Q11, please provide details **in the box below.**	

13. If your NRA is aware of Internet of Things data being collected by fixed or mobile operators in your Member State, can you provide some detail (**in the table to the right**) on the types of service (for example - healthcare, connected cars, wearable devices, household equipment) and the indicators (for example - subscriptions, usage (data volumes), revenues) per service that operators are collecting statistical information on?

Brief description of servi	Who is offering (name/type of operator)?	Sector (residential / business)	Type of indicator	Notes

14. If your NRA has any other additional and relevant information with respect to Internet of Things indicators, not already provided above, please feel free to include such information **in the box below.**

Annex 2: Supplementary questionnaire on IoT indicators

General questions on the importance of IoT indicators for BEREC

1) Why is it important for BEREC to have a common approach with respect to Internet of Things data collection and benchmarking? Please provide your answer in the space below.

2) What statistical indicators on the Internet of Things are important for BEREC to collect data on? Please provide your answer in the space below.

3) Why are these indicators important and why does BEREC need data on such indicators? Please provide your answer in the space below.

Specific questions on spectrum, numbering resources and public security with respect to IoT

4) Is your NRA responsible for the allocation of spectrum? Please provide your answer in the space below.

5) What effects on spectrum policy do you expect the development of the Internet of Things to have, and do you think it's necessary for NRAs/BEREC to monitor these development? Please provide your answer in the space below.

6) Is your NRA responsible for the allocation of other scarce resources (e.g. phone numbers, IMSIs)? Please provide your answer in the space below.

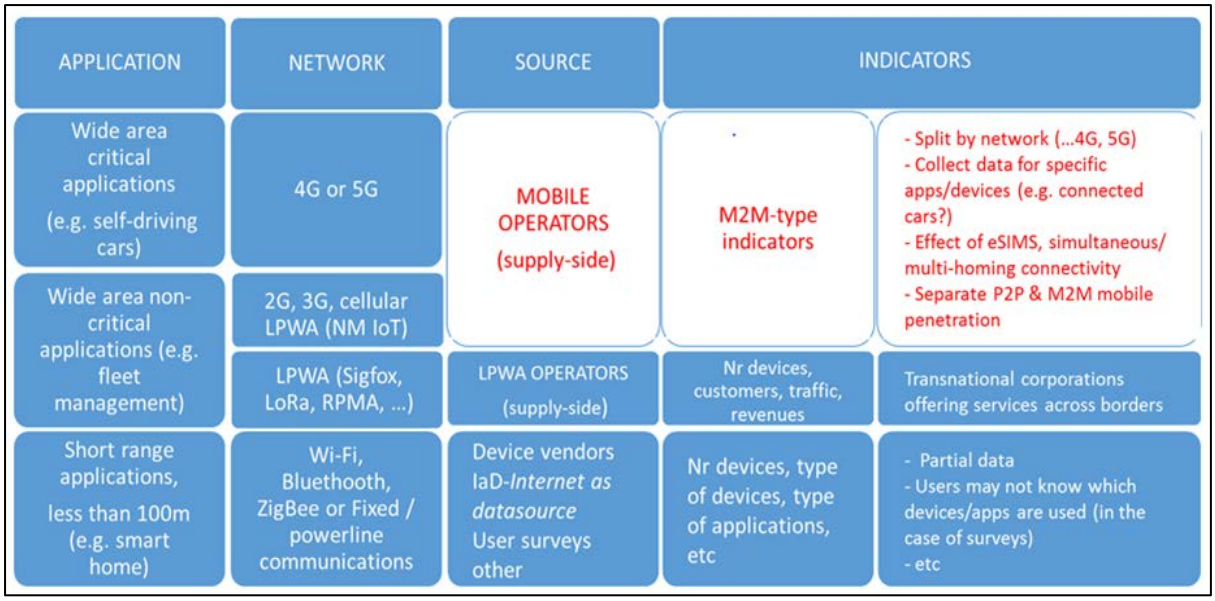
7) With regard to the expected growth in the use of Internet of Things devices, do you see the necessity for NRAs/BEREC to monitor these developments? Please provide your answer in the space below.

8) Do you see the need to monitor which national numbers for Internet of Things devices are used outside your territory (and vice-versa, which numbers assigned in other countries are used in your territory)? Please provide your answer in the space below.

9) For which authorities is this relevant (i.e. is it relevant for NRAs and/or for other national authorities, e.g. authorities responsible for public security or criminal enforcement)? Please provide your answer in the space below.

The "universe of IoT" for BEREC to consider

10) Using the graphic below as a starting point to illustrate the "universe of IoT" for BEREC to consider, with respect to the devices/services/types of access, could you provide any comment in terms of whether you think anything is missing from the illustration, or whether anything could be added? Please provide your answer in the space below.



APPLICATION	NETWORK	SOURCE	INDICATORS	
Wide area critical applications (e.g. self-driving cars)	4G or 5G	MOBILE OPERATORS (supply-side)	M2M-type indicators	- Split by network (...4G, 5G) - Collect data for specific apps/devices (e.g. connected cars?) - Effect of eSIMS, simultaneous/ multi-homing connectivity - Separate P2P & M2M mobile penetration
Wide area non-critical applications (e.g. fleet management)	2G, 3G, cellular LPWA (NM IoT)			
	LPWA (Sigfox, LoRa, RPMA, ...)	LPWA OPERATORS (supply-side)	Nr devices, customers, traffic, revenues	Transnational corporations offering services across borders
Short range applications, less than 100m (e.g. smart home)	Wi-Fi, Bluethooth, ZigBee or Fixed / powerline communications	Device vendors IaD-*Internet as datasource* User surveys other	Nr devices, type of devices, type of applications, etc	- Partial data - Users may not know which devices/apps are used (in the case of surveys) - etc