5 The Internet of Things: data for development

5.1 Overview

Historically, the field of information and communication technology (ICT) has consisted of a wide variety of infrastructural systems, devices and capabilities that were developed and operated independently from one another. In 2005, ITU published one of the first reports on the Internet of Things (IoT) and pointed to the possibility of connecting many new elements to telecommunication networks (ITU, 2005a) Ten years after, the emergent trend and advent of IoT are unifying the various disparate elements of the ICT landscape into a vast yet coherent network of technologies that are capable of communicating and interacting with each other in both anticipated and unanticipated ways.

IoT has the potential to create massive disruptions within the ICT sector — even how the Internet is construed, defined and measured. IoT brings substantial changes to the data/information, computing and ICT domains. Collectively, these changes are having a tremendous societal, technological and scientific impact, and are incorporating many new elements into the information society.

This chapter presents and analyses the various dynamics underlying the rise of IoT. The first section describes IoT, how it is developing, and its relation with ICTs. It then analyses how telecommunication infrastructure is unlocking the potential of IoT and creating opportunities for development, in forms such as new IoT applications and big data generated by the myriad of connected devices. The following section analyses, in more detail, the opportunities that IoT brings to development, paying particular attention to areas of high impact for developing countries, such as health, climate change, disaster management, precision agriculture and the growth of megacities. The chapter concludes by identifying some of the main challenges for the development of IoT and by providing some recommendations on how national statistical offices, telecommunication regulators and ministries can address them.

5.2 Introduction to IoT

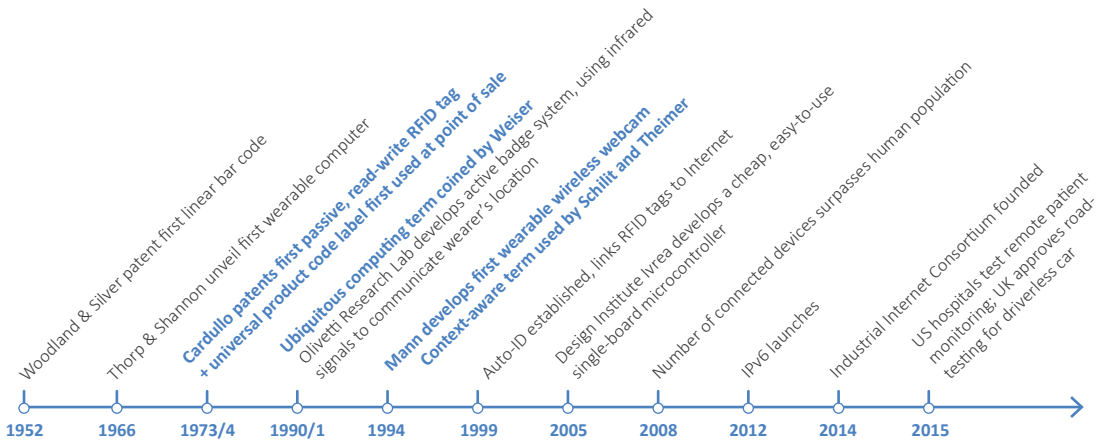
What is IoT?

The ITU Telecommunication Standardization Sector (ITU-T) has defined 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".[1] IoT refers to the burgeoning network of physical objects (e.g. devices) which have an Internet protocol (IP) address for Internet connectivity, as well as the communication that occurs between these objects and other devices and systems that thus become Internet-enabled. The widespread connectivity of devices allows them to share data and exercise control through the Internet, whether directly through their own IP address and ensuing Internet connection or indirectly through other telecommunication protocols, such as WiFi or Bluetooth.

IoT represents a convergence of several factors that have facilitated its growth: growth of the Internet and development of Internet-linked radio frequency identification (RFID), context-aware computing, wearables, and ubiquitous computing, which each developed throughout the second half of the twentieth century, as depicted in Figure 5.1. The sampling of the IoT timeline provides an indication of how extensive the legacy of IoT actually is. The various IoT-related phenomena can also be mapped against an historical backdrop, particularly with respect to the evolution from person-to-person to machine-to-machine communications (Figure 5.2).

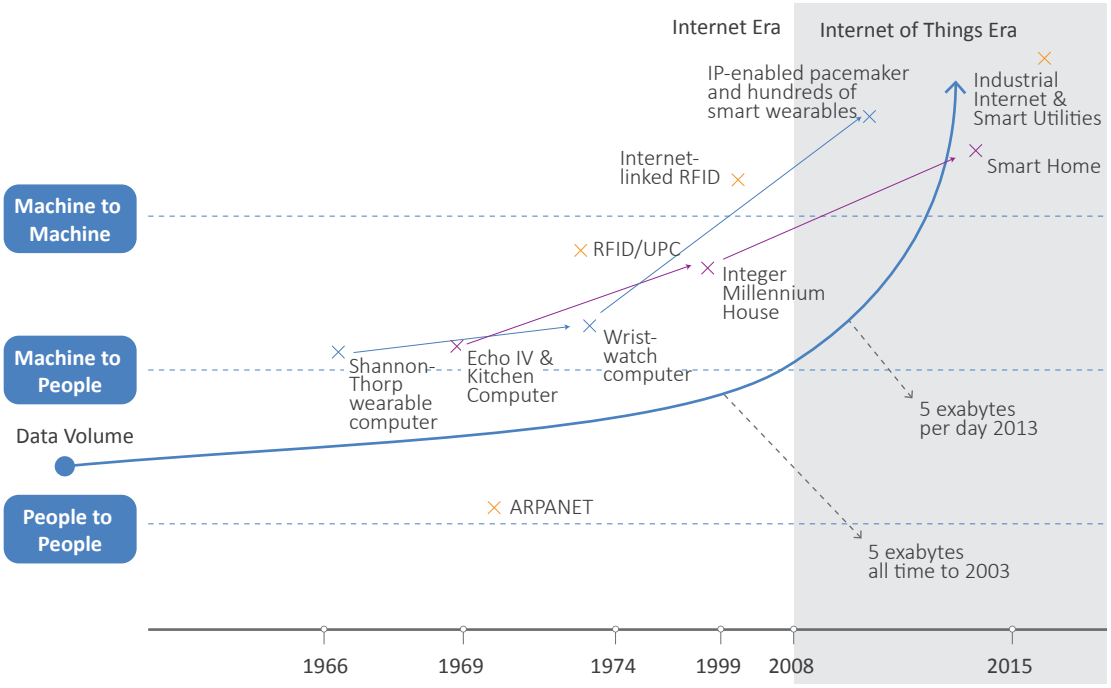
Early Internet-based platforms such as the world wide web (WWW) have been primarily focused on communications between individuals and groups of people, which can be translated into

Figure 5.1: Timeline of developments that led to IoT



Source: ITU.

Figure 5.2: Path to IoT: from people-to-people to machine-to-machine communications



Source: ITU.

person-to-person communications. IoT enables devices to conduct person-to-machine as well as machine-to-machine (M2M) communications without human intervention (Chen, 2012). A subtle but distinguishable characteristic of the M2M subdomain within IoT is worth noting: whereas M2M refers specifically to "things" (i.e. devices, machines, or anything that can send data) connecting to other "things" (e.g. remote computer) so as to form isolated systems of sensors and islands of telemetry data, IoT also encompasses "things" connecting with people and systems.

IoT represents a step forward in the connectivity provided by M2M connections, because it offers the potential for integrating disparate systems and enabling new applications. Indeed, M2M communication capabilities are seen as an essential enabler of IoT, but represent only a subset of its whole set of capabilities. From this point of view, IoT can be construed as the arch connecting M2M vertical pillars[2] (i.e. technology stacks), and for IoT to provide value that extends beyond M2M it must fulfill a function not already addressed by an individual M2M stack.

More specifically, M2M communications, particularly in the context of ICT infrastructure, are often referred to as "plumbing", while IoT is deemed to be a universal enabler, as it extends beyond M2M communications to include information exchanges between people, and between people and devices. Devices within the M2M paradigm typically rely upon point-to-point communications (i.e. communication between a "thing" and a remote "thing") and use embedded hardware modules (e.g. subscriber identity module or SIM card).

In many cases, devices within the IoT paradigm rely upon standards-based IP communication networks; however, it is important to note that devices within M2M do not rely solely upon the prototypical TCP/IP over Ethernet for connectivity (Kim, 2011). Whereas emerging wireless broadband platforms are contributing to the growth of IoT connectivity, technologies such as Bluetooth (Miller, 2000), ZigBee (Baronti, 2007), and other protocols/standards enable devices to communicate and are increasingly used in IoT implementations. For example, the ZigBee protocol works with the IEEE 802.15.4 standard, which specifies the physical layer and media access control for low-rate wireless personal area networks. As another example, while Z-Wave[3] implementations are in accordance with the Recommendation ITU-T G.9959, each individual vendor's implementation can vary for the protocols used in the transport layer.

IoT uses various protocols/standards to accommodate low-power and passive sensors as well as other inexpensive devices that might not be able to justify a dedicated M2M hardware module. In addition, IoT-based delivery of data is, typically, to a cloud-based architecture, thereby allowing IoT to be inherently more scalable. In essence, devices that are not directly IP-addressable are leveraging wireless radio protocols/standards so as to indirectly connect to the Internet, and thus the rising volume of M2M communications is contributing to the growth of IoT (Goodwin, 2013). However, IoT shares some of the regulatory challenges of M2M, such as the lock-in of M2M subscriptions with a single operator, particularly when considering cross-border communications (Box 5.1).

As devices are endowed with communication capability, they can make their own contributions to IoT (Gantz, 2008). IoT is by no means a singular class, or standardized set of devices. Just as there is a wide variety of connected device types, these various devices exhibit a range of connectedness (Figure 5.3). By way of example, even though personal wearable devices, such as for calculating

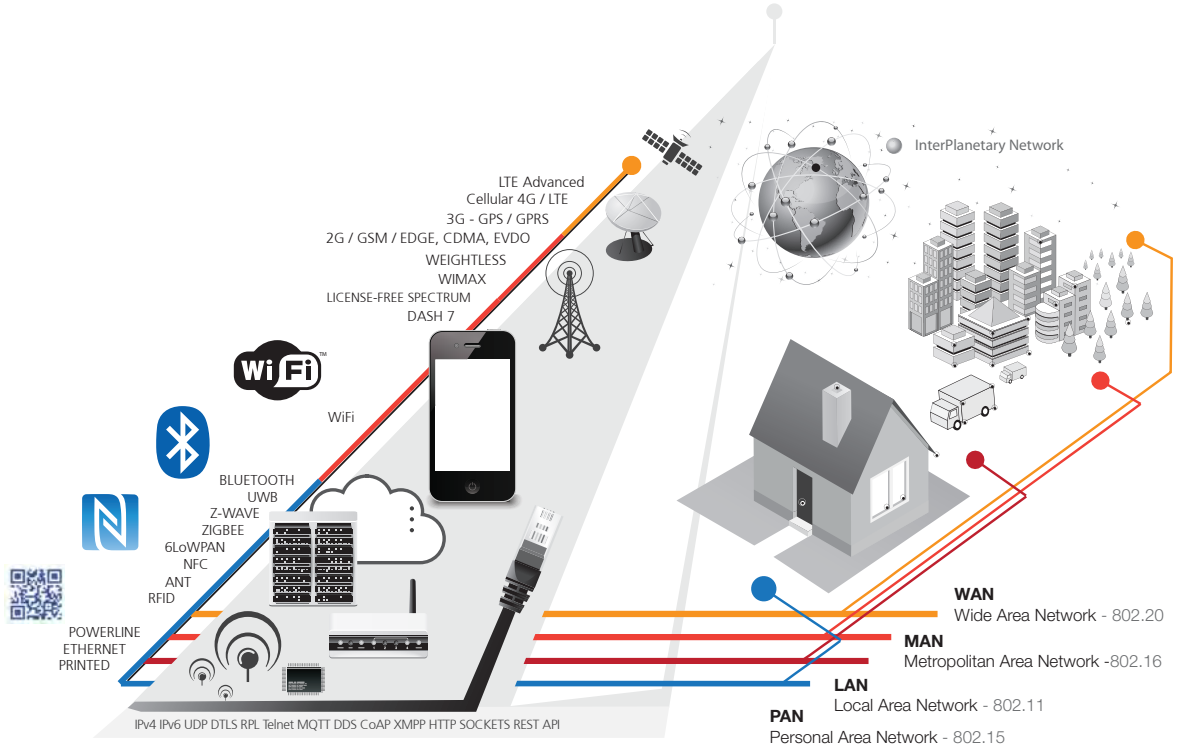
Box 5.1: IoT communications across borders

The manufacturing of devices with IoT capabilities — in industries with large volumes — is usually managed at the global level, in order to take advantage of the economies of scale and scope that the outsourcing of production allows. For example, in the automotive industry, cars that are manufactured in a given country with embedded M2M capabilities are sold and used in several foreign markets, and the same occurs in most sectors in which IoT can make an impact.

Although the production of devices with embedded IoT capabilities has become global, pricing of the actual IoT communications remains local. For instance, if a truck with an embedded sensor travels from one country to another – which is, for instance, often the case in the European Union – the information sent by the sensor to the Internet will be subject to roaming charges. Considering that roaming rates are significantly higher than regular mobile prices (see Section 4.5), this may limit the use of the IoT capabilities embedded in the truck. A similar situation will arise if a person with an e-reader travels to a foreign country and wants to download a travel guide from the Internet using the SIM card embedded in the e-reader.

The limitations that roaming charges place on the development of M2M have been extensively discussed, as have the possible regulatory actions that could mitigate them (OECD, 2012). As the industry advances from M2M to IoT and the need for affordable cross-border connectivity grows, this issue will require more regulatory and policy attention.

Figure 5.3: Diagram of IoT connectivity



Source: Postscapes and Harbor Research, http://postscapes.com/what-exactly-is-the-internet-of-things-infographic.

the number of steps taken, etc., are capable of collecting data, they rely upon additional communication gateways (e.g. smartphone, laptop) to transmit these data to a cloud-based application (Desai, 2014). Indeed, many wearables do not have their own Internet connection and must wait until they are in range of Bluetooth connectivity or similar connective networks. In essence, devices can be classified as either: (1) having their own Internet connection with capability of accessing the Internet at any time; or (2) dependent upon a network with connection to the Internet. IoT encompasses both (Want, 2015).

The development of IoT fosters the creation of wireless sensor networks (WSNs, Box 5.2), and this may lead to the development of alternative network architectures. Today, in the usual network configuration, mobile data pass through the carrier's gateway to connect to the Internet (Pitoura, 2012), and most mobile devices are thus connected to the Internet (Dinh, 2013). Researchers have been exploring communication approaches that could potentially bypass the Internet entirely by facilitating peer-to-peer communication between WSN clusters so as to form a new "Internet" comprised of WSNs (Xu, 2005). As people opt in to allow their wireless personal area networks to communicate with WSNs, communication can occur directly between WSNs rather than through the traditional Internet.

Apart from WSNs, there is another potential technological disruption on the horizon. Semiconductor companies are advancing system on chip (SOC) (Wolf, 2008) paradigms tailored for IoT. Intel, Broadcom and ARM have all developed SOC for the IoT market. In essence, connected devices are becoming smarter with higher-performance embedded processors as well as increased memory and random access memory (RAM) as the per unit cost of SOC and storage continue to drop and components become more miniaturized (Itoh, 2013). While SOC is not something that has just been developed, the advent of programmable SOC (PSoC) marks a new era of longevity and extensibility. This has particular potential to change the IoT paradigm.

To articulate this point, during the fourth quarter of 2014 a new PSoC for IoT was unveiled at the Electronica international trade show in Munich, Germany (Bahou, 2014a). This unveiling was particularly interesting, as it moved beyond the

Box 5.2: Wireless sensor networks

In essence, a WSN is a network formed by a large number of sensor nodes, wherein each node is equipped with a sensor to detect physical phenomena (e.g. light, vibration, heat, pressure, etc.) (International Electrotechnical Commission, 2014). WSNs exist in various domains ranging from electric grids and other critical infrastructure to building management and transportation. The power industry has been upgrading various parts of the electric grid, and WSN technologies are playing an important role for a smarter grid, including online monitoring of transmission lines, intelligent monitoring and early warning systems for distribution networks, and smart electricity consumption services (Eris, 2014). As these WSNs, which are deemed to be a revolutionary information-gathering method, are increasingly becoming a critical part of the ICT infrastructure that underpins the reliability and efficiency of infrastructure systems, they are becoming the key technology for IoT[4](Khalil, 2014). In managing energy consumption in green buildings, WSNs can be implemented to control the illumination of homes and offices, thereby minimizing the power wasted by unnecessary lighting in vacant rooms and office spaces (Magno, 2015). In the context of smart cities, WSNs are being used to design traffic monitoring and control systems that go beyond the conventional round-robin scheme of reducing congestion at busy intersections, by dynamically prioritizing higher volume lanes of traffic (Desai, 2014). With regard to critical infrastructure protection and public safety, WSNs are also being widely employed in the detection of hazardous gas leaks (Somov, 2014). Although these areas represent only a glimpse of the many ways WSNs are being employed, such a diversity of applications demonstrates how transformative this technology is likely to be. As an example, urban consolidation centres (UCCs) can reduce the traffic load caused by delivery vehicles. By having the UCC warehouses geographically situated just outside the city, goods destined for retailers in the city are first consolidated and then shipped with an optimized routing, thereby making the best possible use of truck capacity and reducing the total number of trucks needed. For this paradigm, tracking at the pallet (or other packaging unit) level is required. The pallet becomes the "sensor" for measuring the flow of goods, and a combination of various wireless technologies (e.g. GPS, RFID, WLAN, cellular) in combination with big data analysis techniques are utilized to optimize scheduling and routing.

typical trending of decreasing size, cost and energy consumption and presented a PSoC that was not only scalable, but also extensible. In other words, the PSoC was "future-proofed," enabling firmware-based changes at any point in the design cycle, including after deployment. It also showcased the possibilities of single-chip Bluetooth® low energy (BLE) PSoC for IoT: home automation, healthcare equipment, sports and fitness monitors and other, wearable smart devices.

Similarly, a BLE programmable radio-on-chip presents a viable method for wireless human interface devices, remote controls and other applications requiring wireless connectivity (Bahou, 2014b). As research progresses into developing increasingly compact PSoC designs that can harvest energy as well as sense and communicate a variety of data wirelessly, the limits of IoT capabilities will continue to extend (Klinefelter, 2015).

The importance of IoT and its potential to become a disruptive technology has been recognized by several administrations and organizations. For instance, in 2008, the United States National Intelligence Council identified IoT as one of the six primary "disruptive civil technologies" that will most significantly impact national power through 2025 (NIC, 2008). This particular assessment of IoT is well captured in a 2009 speech by the Chinese Premier, who presented the equation: *Internet + Internet of Things = Wisdom of the Earth.*[4] Similarly, Cisco asserts that IoT is the next evolution of the Internet, and this transformation occurred during the 2008-2009 time period when the number of objects connected to the Internet surpassed the number of people online worldwide (Evans, 2011). The United Kingdom Government, in its 2015 budget, made quite the statement by allocating GBP 40 million to IoT research (Gibbs, 2015).

Today, it is estimated that over 50 per cent of IoT activity is centred on manufacturing, transportation, smart city and consumer applications, but that within five years all industries will have rolled out IoT initiatives (Turner, 2014). Indeed, IoT will have a significant impact on nearly every industry of our society, revealing and making possible new business models and workflow processes as well as new sources of operational efficiencies. A key element in reaching the efficiency gains that IoT can deliver will be interoperability within vertical industries (i.e. across different manufacturers in the same industry) as well as across industries. Indeed, it is estimated that the interoperability of IoT systems is the key to unlocking 40-60 per cent of potential value across IoT applications (McKinsey, 2015).

IoT will very likely revolutionize how individuals, corporations, government and international organizations interact with the world. Whereas IoT centres upon connected devices that enable the range of capabilities shown in Figure 5.4, it is by no means the end of the line for technological evolution. Researchers, industry experts and technologists foresee an evolutionary path beyond IoT to an Internet of Everything (IoE), in which communications among people, devices, data and processes will be fully unified (Bradley, 2013).

What is the role of ICTs in IoT?

ICTs comprise a broad and unconsolidated domain (Lampathaki, 2010) of products, infrastructure and processes (Antonelli, 2003)

Figure 5.4: Sectors in which IoT can play an enabling role for development

Source: ITU based on Al-Fuqaha, Ala *et al.* (2015).

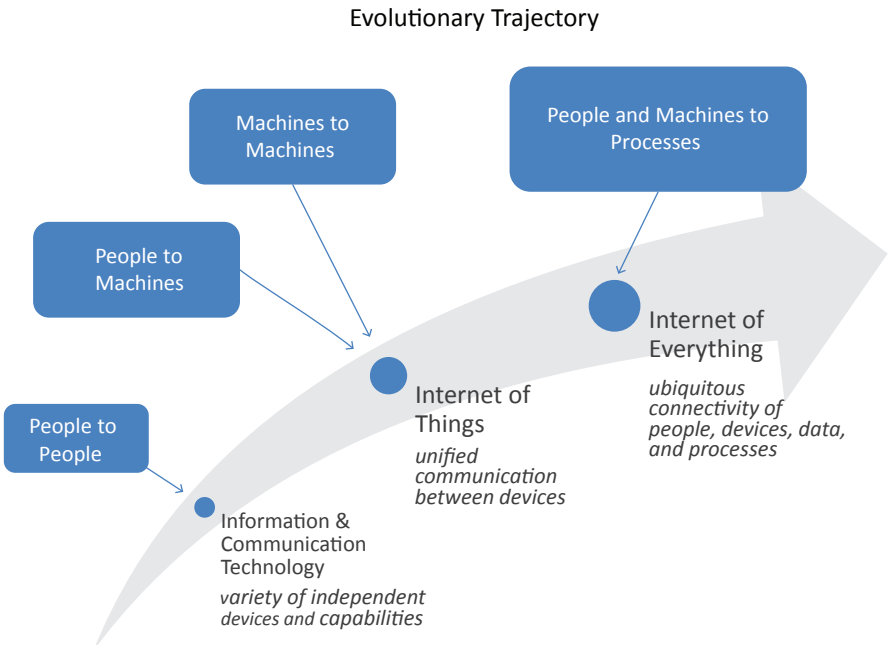
that include telecommunications and information technologies, from radios and telephone lines to satellites, computers and the Internet (Riemer, 2009). In turn, IoT is composed of objects that communicate, via the Internet or other networks, which might not be identified as ICTs in the conventional sense (Nambi, 2014). On one hand, the advent of IoT represents an evolution of ICTs (Roselli, 2015); on the other, ICTs are key enabling technologies, without which IoT could not exist (Gubbi, 2013). The IoT world is indeed underpinned by ICT infrastructure, which is needed to gather, transmit and disseminate data as well as facilitate the efficient delivery of services for society at large (e.g. health, education) and assist in the management of organizations, whether it be for individuals, companies, governments or international organizations. ICTs serve as an enabler for individual social development and societal transformation by improving access to critical services (including by way of IoT pathways), enhancing connectivity and creating new opportunities.

Robust ICT infrastructure can most definitely facilitate — at the very least — the transmission of a greater volume, variety and velocity of data; these three "V"s in particular collectively serve to better allow for in-stream processing and analytics so as to help "remove hay from the haystack" (Lindquist, 2011) and better illuminate the "needles in the haystack" (Grover, 1997). With this foundational basis, the veracity of data can be better scrutinized, and, playing a role similar to that of traditional "small data" (Martens, 1998) in verification, relevant long-tail data from the entire corpus of devices may prove extremely illuminating in providing maximum context in terms of validating information (i.e. to mitigate against misinformation or disinformation) and providing an additional value-added proposition for the community at large.

A higher level of confidence in ICT infrastructure and its capacity to ensure data privacy and protection will lead to an ever-increasing reliance on IoT. Likewise, this reliance on IoT will serve as a self-reinforcing societal trend for an even more ubiquitous IoT, thereby eventually leading to the IoE phenomenon that will extend connectivity beyond the boundaries of IoT and connect people, processes, data and things (Evans, 2012), as depicted in Figure 5.5.

Although aspirational, IoE could result in networks of networks with trillions of connections, facilitating automated connectivity, embedded intelligence and event correlation (Yesner, 2013). Whereas IoT connects objects to the Internet so as to increase available data in a query-response paradigm, the envisioned IoE will enable greater automated insight generation in a real-time sense-

Figure 5.5: Evolution from the Internet of Things to the Internet of Everything



Source: ITU.

and-respond paradigm (Etzion, 2014) through computational capacity in the cloud and within objects themselves (Kiat Seng, 2014). At the very least, the notion of IoE helps to position and establish an envisioned approach for architecting next-generation systems and devising viable policies to contend with the massive torrent of big data.

The IoT and big data

More big data have been generated, especially via IoT, during the last 2 years than in all of previously recorded history (Sagiroglu, 2013). Table 5.1 presents a range of estimates from a variety of sources regarding data generated and stored in electronic format, and Table 5.2 compiles estimates on the size of IoT and its potential value.

Table 5.1: Summary of statistics on global data generated and stored in electronic format

Data generated		
Indicator	**Statistics**	**Source**
Total data generated:	From the dawn of civilization to 2003, humanity has generated 5 exabytes (EB) of data	Intel (2013)
Data structure:	85% of big data is unstructured	Berry (2012)
Genomic data per person:	4 terabytes (TB)	Miller (2012)
Data generated by Boeing jet engine per 30 minutes of flight:	10 TB	Higginbotham (2010)
Data generated by automobile per hour of driving:	25 gigabyte (GB)	Taveira (2014)
Data increase in electrical utilities due to IoT-enabled smart grid:	680 million smart meters will be installed globally by 2017. This will lead to 280 petabytes (PB) of data per year.	Bloomberg (2015)

Data in electronic format		
Statistics		**Source**
The volume of data stored in electronic format has been doubling almost every 18 months.		Gantz (2011)
2013	3.1 zettabytes (ZB) data centre traffic	Cisco (2014)
	4.4 ZB (trillion gigagbytes) total	Gantz (2011)
	5 GB per capita	Bahrami (2015)
2014	2.5 billion GB per day; 1.7 megabytes (MB) per minute per capita	Gantz (2011)
2015	14.5 billion indexed webpages	Woollaston (2013)
2016	1 ZB global annual IP traffic	Cisco (2015)
2018	403 ZB total IoE traffic	Cisco (2014)
	14 GB per capita	Bahrami (2015)
2019	2 ZB global annual IP traffic	Cisco (2015a)
2020	44 ZB (44 trillion GB)	Gantz (2011)
	10% from embedded IoT devices	Gantz (2011)
	27% from mobile connected things	Gantz (2011)

Note: data volumes are expressed in multiples of bytes: kilobyte (1024), megabyte (1024^2), gigabyte (1024^3), terabyte (1024^4), petabyte (1024^5), exabyte (1024^6) and zettabyte (1024^7).

Table 5.2: The size and value of the Internet of Things in numbers

Size of IoT		
Indicator	**Statistics**	**Source**
Number of connected devices, milestones reached:	70% annual growth in sensor sales since 2002	Evans (2011)
	2008-2009: Number of global connected devices surpasses human population	Gartner (2013)
Number of connected devices today:	8 billion devices or 6.58 devices per person online	Cisco (2015b)
Number of connected devices by 2020:	Nearly 26 billion devices will be connected as part of IoT by 2020 (and this figure excludes smart phones, tablets and PCs, which would account for another separate 7.3 billion devices)	Gartner (2013)
	More than 30 billion devices will be connected by 2020	ABI (2013)
	Approximately 50 billion devices will be connected by 2020 (CISCO)	Evans (2011)
	75 billion devices will be connected by 2020 (Morgan Stanley)	Danova (2013)
	Anywhere from 50 to 100 billion devices will be connected by 2020 (Bell Labs)	Trappeniers (2013)
	The number of devices is already approaching 200 billion (IDC)	Turner (2014)

Potential value of IoT		
Indicator	**Statistics**	**Source**
IoT incremental revenue by 2020:	USD 300 billion, mostly from services	Gartner (2013)
IoT market worth by 2020:	USD 7.1 trillion	Press (2014)
IoT annual growth of market worth by 2025:	USD 3.9-11.1 trillion, 40% generated in developing countries	McKinsey (2015)
IoT contribution to GDP over the next 20 years:	USD 15 trillion	Press (2014)
IoT by sector:	50% of IoT activity is centred around manufacturing, transportation, smart city and consumer applications	IDC (2011)

Note: data volumes are expressed in multiples of bytes: kilobyte (1024), megabyte (1024^2), gigabyte (1024^3), terabyte (1024^4), petabyte (1024^5), exabyte (1024^6) and zettabyte (1024^7).

The number of connected devices

Big data are being created by billions of devices around the world, as shown in Table 5.1. It is estimated that from 26 to 100 billion devices (Gartner, 2013) (Trappeniers, 2013) (ABI, 2013) will be connected as part of IoT by 2020. These devices will include the traditional "dumb" devices (e.g. toaster, light bulb, refrigerator, faucet), which will be made "smart" with real-time sensors equipped with communication capabilities.

In addition to these devices, many additional, hitherto unconnected consumer devices and industrial machines could be connected to the Internet, and this number (particularly in the realm of sensors) is burgeoning. There are multiple factors "accelerating the data surge" (Press, 2014), including:

(1) Increased affordability: technological progress, such as high-volume manufacturing techniques, and the increase of the size of the market of devices with embedded communication technology allow for economies of scale; the 70 per cent annual growth in sensor sales since 2002 (Gartner, 2013) is leading to a situation in which ever-more capable sensors are becoming more affordable.

(2) Increased connectivity, access to cloud computing (Zhang, 2010) and more affordable high-speed wireless data networks extend the

reach of IoT applications to uses not yet even imagined.

(3) Rapid innovation: technological advances make it possible to include multiple sensors within one device to perform a variety of distinct and disparate tasks (e.g. detecting geolocation, temperature, motion, etc.); furthermore, power management is allowing devices to run unattended for longer periods of time (Abras, 2008).

(4) Regulatory mandates and policy initiatives are accelerating the adoption rate of IoT solutions, especially within industries (e.g. healthcare, automotive and energy). As just one example, the European Union has mandated that 80 per cent of European homes must have a smart meter installed by 2020 (Faruqui, 2010).

(5) The adoption of communication protocols, such as Internet Protocol 6 (IPv6), allows more devices to connect to the Internet; IPv6 has 2^{128} addresses as compared with 2^{32} for IPv4 (Wu, 2013).

(6) The high expectations that IoT is generating in industrial markets are encouraging more stakeholders to enter the IoT market, thus contributing to increasing the number of devices and expanding the sector. Indeed, industrial titans such as General Electric are forecasting that the industrial Internet has the potential to contribute approximately USD 15 trillion to global GDP over the next 20 years (Press, 2014), and connected cars, smart homes, wearables, *et al.*, are expected to comprise trillion dollar markets (MacGillivray, 2013).

In this context, it is possible to imagine several scenarios that may be close to becoming reality. For example, a home camera device detecting movement of a pet can notify the homeowner, via an e-mail or text message; it can capture the associated video and transmit the video stream to a private cloud. Should the homeowner elect to share the video – let us say that the movement by the homeowner's pet and the associated video has the potential of being propelled to the ranks of YouTube's funniest videos – then that video will be transmitted, disseminated, propagated, replicated and preserved in archives and repositories all over the world. Screen captures and textual transcriptions of the video — and related data — can be shared, via social networking platforms, microblogging platforms and other social media platforms.

The torrent of big data from connected devices

As connected devices create new opportunities for the scientific exploration of large datasets, there is an increasing volume of and value given to observational, experimental and computer-generated or machine-spawned data. In the context of big data, human-generated data (e.g. textual data – e-mails, documents, etc.; social media data – pictures, videos, etc., and other data) represent an increasingly diminishing percentage of the total; after all, IoT devices are producing machine-generated data (e.g. remote-sensing data – volcanic, forestry, atmospheric, seismic, etc.; photographs and video – surveillance, traffic, etc.) and sharing them directly with other devices without any human intervention.

Given the sheer volume of human-generated as well as machine-generated data, there have been several attempts to quantify these data and project future trends. The 2014 report of the *EMC Digital Universe Study* asserts that, as a result of IoT, the amount of data generated in digital format is doubling every two years and will increase by about a factor of ten between 2013 and 2020 – from 4.4 trillion gigabytes to 44 trillion gigabytes (IDC, 2011).

The 2013 4.4 ZB estimate of the data generated in digital format breaks down into 2.9 ZB generated by consumers and 1.5 ZB generated by enterprises.[5] In fact, only 0.6ZB (about 15 per cent) of the consumer portion is not touched by enterprises in some way, leaving enterprises responsible for the vast majority of the world's data (about 3.8 ZB in 2013),[6] with mobile connected things contributing another 27 per cent[7]. In terms of geography, EMC and IDC predict that the balance will swing from mature markets, which accounted for 60 per cent of the data generated in digital format in 2013 (Turner, 2014), to emerging markets within developing countries, with the inflection point occurring around 2016-2017 (Turner, 2014). This nevertheless presumes that the infrastructure in the emerging markets of developing countries will be able to cope with this increase in enterprise data, which would require major investments in ICTs.

In this world of big data, several latent data sources are starting to be tapped. For instance, each person equates to about 4 TB of raw genomics data (Miller, 2012), a Boeing jet generates 10 TB of information per engine for every 30 minutes of flight (Higginbotham, 2010), and the array of sensors in a modern hybrid car generates 25 GB of data per hour of driving (Taveira, 2014). Given the aforementioned genomic, jet engine and automotive examples, the descriptor "torrent of data" (Vermesan, 2011) — to represent the phenomenon of big data being generated and shared among connected devices — is difficult to dispute. To accompany this "torrent of data", there are data given off as a byproduct (Singh, 2014). This "digital exhaust" is both actively contributed (e.g. the writing of a blog post) and passively contributed (e.g. the background generation by the device — mobile phone or other — of geolocation, time, date and other metadata).

It is important to note that, currently, most of the world's data are transient (e.g. the streaming video of Netflix Instant, Hulu Plus or Amazon Instant Video, etc.) and require no storage. The significance of this resides in the fact that the global amount of available storage capacity (i.e. unused bytes) across all media types is growing at a much slower rate than the data generated in digital format (Hilbert, 2011). In 2013, the available storage capacity could accommodate just 33 per cent of the data generated in digital format (Turner, 2014). By 2020, it is forecast that it will be able to store less than 15 per cent of such data (Turner, 2014). In essence, the amount of data being generated is far outpacing the ability to store those data, let alone analyse them (Kumar, 2011).

The volume of data produced by connected IoT devices is a problem not only of storage, but also of sustainable access and preservation. The diversity of data formats, metadata (all of which might not necessarily adhere to metadata standards, such as the Dublin Core Metadata Standard), semantics, access rights, associated computing hardware, and the myriad of software tools for modeling, visualizing and analysing the data too, collectively, all add to the complexity and scale of the big data challenge.

In addition, the vast amounts of data that will be generated by IoT devices will put enormous pressure on networks and data centre infrastructures. IoT data flows will be primarily from sensors to applications and will range between continuous data flows (e.g. real-time stock ticker system) and bursty data flows (e.g. non-real-time video) depending upon the type of application. The anticipated magnitude of IoT-related network connections and data volumes is likely to favour a distributed approach for data centre architectures, with several "mini-data centres" performing initial processing and forwarding relevant data over wide area network (WAN) links to a central data centre for further analysis.[8] Cisco has coined the term "fog computing" (Bonomi, 2012) to describe this methodology of data processing at the network edge or "edge computing" so as to mitigate against location-based and/or network latency issues. The efforts to back up this massive volume of data will accentuate issues of remote storage bandwidth and potentially insufficient storage capacity.

The examples given in this section show how IoT is shaping the observational space for what is considered "useful data." In 2013, according to Turner (2014), only 22 per cent of the data were considered useful, and less than 5 per cent of that "useful data" were actually analysed. By 2020, more than 35 per cent of all data could be considered "useful data" due to the strategic and tailored growth of data from IoT, but it will be up to the community at large to determine what are "useful data" and come up with methodologies to actually put these big data to use.

Regardless of whether data are deemed to be "useful data" or "not useful data" (incidentally, some type of analysis would be required to make this initial determination), there is most definitely a great deal of data traffic. Commercial traffic through large data centres for business applications represents a significant portion of the data generated in digital form (Benson, 2010) Yet despite the potential invaluable commercial value of the data, less than 1 per cent of that data has actually been analysed (Box 5.3) (Burn-Murdoch, 2013).

To explain this situation, it is worthwhile to note that many early instances of connected devices have occurred in the context of private internal networks, or "intranets of things", which were developed and operated in isolation from industrial-scale commercial applications (Zorzi, 2010). Although such internal networks

Box 5.3: Surface web and deep web

The surface web is that part of the world wide web (WWW) that is readily available to the general public and searchable by traditional search engines. From a quantitative point of view, it maintains a current steady contribution of approximately 571 websites per minute per day toward the already existing corpus of about 14.5 billion indexed webpages.[9] Apart from this indexed set of webpages, Google estimates that WWW is growing at a speed of about a billion pages per day.[10] Moreover, according to YouTube, more than 300 years' worth of video are uploaded to digital video repositories daily, and the substantive portion of the corpus of YouTube videos on the surface web has not yet been analysed.

The deep web is that part of WWW that is not readily available to the general public and cannot be indexed by traditional search engines. By way of background information, web crawlers collect and index metadata (e.g. page title, URL, keywords, etc.) from every site on the surface web, which constitute far less content than that of the actual site. Pages on the deep web function in the same way as any surface website, but are built in such a way that their presence is not readily discoverable by a web crawler for any of several reasons. First, search engines typically ignore pages whose URLs consist of lengthy sequences of parameters, equal signs and question marks in order to avoid duplication of indexed sites. Second, web crawlers cannot access sites with form-controlled entry (i.e. page content only gets displayed when an actual person applies a set of actions and databases generate pages on demand, such as flight information, hotel availability, job listings, etc.) or sites with password-protected access, including virtual private networks (VPNs). In addition, sites with timed access (i.e. free content becomes inaccessible after a certain number of page views, and is moved to a new URL requiring a password) and robots exclusion (i.e. a file in the main directory of a site tells search robots which files and directories should not be indexed) are inaccessible to web crawlers. Finally, there are hidden pages that no sequence of hyperlink clicks could navigate to, and therefore are only accessible to individuals who know of their existence.[11]

Initial research on the size of the deep web found that it was approximately 500 times greater than the surface web (i.e. the deep web contained nearly 550 billion individual documents compared with about one billion on the surface web (Bergman, 2001)), and sixty of the largest deep web sites collectively contained about 750 TB of information — sufficient by themselves to exceed the size of the surface web forty times over (Bergman, 2001). Subsequent research on the deep web has been carried out applying surveying techniques, such as random sampling of IP addresses or hosts, to estimate the size of the deep web. The results have revealed additional deep web data sources suggesting that the deep web might be larger than initially thought (B. He et al., 2007; Madhavan et al., 2007; Shestakov, 2011). Although research on the quantification of the deep web is ongoing, it has been established that the deep web has as much as an order of magnitude more content than that of the surface web (He, Yeye, et al., 2013) and that the deep web is the largest-growing category of new information on the Internet (B. He et al., 2007).

or intranets have generated vast amounts of data, these repositories are not accessible on the public Internet. In light of the vast amount of personal data that can be collected by wearables as well as home networking devices, maintaining isolated intranets of things separate from the public Internet is a vital consideration in terms of understanding how much data are being segregated due to desired privacy and securing the privacy of sensitive data (Roman, 2011).

5.3 The opportunities of IoT for development

IoT offers new opportunities for development by providing a new data source that can contribute to the understanding, analysis and tackling of existing development issues. As a consequence, the debate on IoT has become part of the larger debate on the data revolution and the possibilities that new ICT developments (including the growth of IoT)

have opened up to achieve larger development goals, including those addressed by the new Sustainable Development Agenda.

The potential overall economic impact of IoT is profound, and while estimates vary, McKinsey expects the IoT market to generate from USD 3.9 trillion to 11.1 trillion a year by 2025 (McKinsey, 2015). The latter figure is roughly equivalent to 11 per cent of the global economy. Keeping this in mind, while over the next ten years IoT may indeed potentially represent a higher value within advanced economies based on higher value per use, it is anticipated that nearly 40 per cent of its value will be generated in developing economies (McKinsey, 2015). Hence, the future of leveraging IoT for developing countries is quite promising. While many discussions on the opportunities offered by IoT have focused on the consumer side and benefits for the individual, IoT offers great potential for broader development issues. Existing examples of the use of IoT for development are mainly to be found in the areas of health, climate change and disaster management, water and sanitation, and agriculture and infrastructure. IoT has been recognized as providing a particular opportunity to address challenges faced by the growing number of megacities, and to help turn cities into smart cities.

The following section will look into some of the uses of IoT to address certain key challenges facing developed and developing countries. It will highlight the fact that there are significant global development challenges that IoT can potentially help to address. In fact, IoT can well serve as a launching pad for developing countries in contending with epidemics and natural hazards and managing resource scarcity. IoT-centric endeavours also include precision agriculture for the production of food, tests for water quality, and systems that relate to the provision of public services to residents, such as transportation. The rise of IoT offers developing nations the potential to leapfrog and accrue especially large benefits from strategic technological adoption (Nolan, 1985). Emphasis will be placed on the discussion of megacities, for megacities concentrate and exacerbate several challenges found on a lesser scale elsewhere. Indeed, megacities can serve as testbeds for IoT applications aimed at alleviating key issues, particularly those centred around basic infrastructure services such as energy, water, sewage disposal and sanitation.

IoT for health

An important role for IoT has been established in the area of healthcare delivery, research and response. From the advent of wearable health devices and other sensor-based capabilities to the monitoring of pandemics and endemic disease control, the opportunities within the IoT paradigm are growing. A macro-level approach to combining anonymized user data allows a more comprehensive view of the observational space, and layering additional datasets, such as geographic or economic, can provide additional insight. For example, today's amalgam of mobile-cellular data and other sensory data from IoT might shed more insight into the cyber-physical supply chain at hand and provide a test of reasonableness regarding data validity — for tracking, anticipating and mitigating the spread of infectious disease.

This notion of IoT syndromic surveillance (i.e. the collection and analysis of health data pertaining to a clinical syndrome that has a significant impact on public health), especially for the purposes of potentially modeling the spread of infectious diseases, has already been used to great effect (Wesolowski *et al.*, 2012). For example, in Kenya, passive mobile positioning data was combined with epidemiological data to identify the prevalence, spread and source of malarial infections (Wesolowski *et al.*, 2012, 2015). Similar experience in Haiti also illuminated how mobile positioning data could be used to study both population displacement and the spread of cholera after the 2010 earthquake (Rinaldo, 2012).

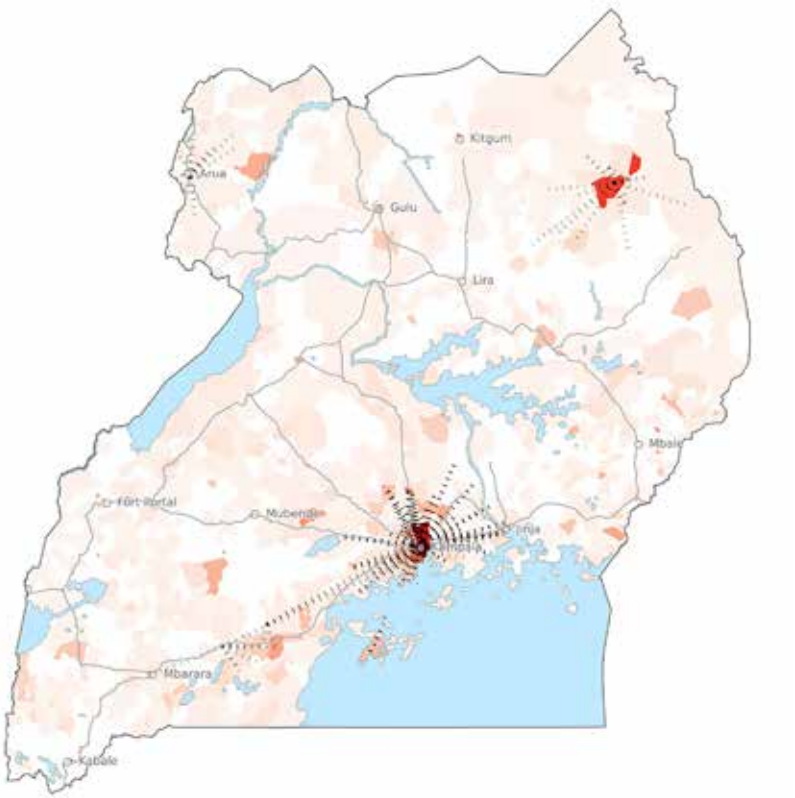
Most recently, mobility data were used during the Ebola outbreak in several West African countries (Fink, 2015), and highlighted the need for more extensive and timely data for pandemic disease tracking and prevention. Population flow data between areas is a key ingredient in Ebola containment strategies, and analysis of travel routes is the best resource (Wesolowski *et al.*, 2014). As a mobile phone subscriber moves from one area to another, the phone will ping towers along the way. It is often difficult to obtain such granular data, thus policies for sharing aggregated and anonymized datasets are encouraged. Companies like OrangeTelecom made such data available during the Ebola crisis.

ITU, in cooperation with the Government of Sierra Leone and the operators in the country, is carrying out a project to analyze anonymized call detail records to understand geographic mobility patterns of communities affected by the Ebola outbreak. In a similar approach, the UN Global Pulse Lab, along with the Ministry of Health in Uganda and WHO, is carrying out infectious disease and risk factor mapping in Uganda through advanced data visualization techniques (UN Global Pulse, 2015). The conjoining of mobility data with remote sensing and geographic information systems (GIS) data offers great potential for tracking the spread of infectious diseases and the deployment of resources (Figure 5.6).

IoT has the inherent potential to improve upon scientific concepts related to epidemic studies. In 2015, for example, Microsoft began testing semi-autonomous drones whose purpose is to carry a trap to collect mosquitoes in remote areas. These mosquitoes will be utilized in the lab to identify the prevalence of diseases such as avian flu and dengue fever. The method circumvents what is currently a painstaking and lengthy process to obtain samples, ultimately reducing the latency of deployment of pesticides or other control methods (Linn, 2015). In the future, rural communities will be able to have test results in minutes from a sample collected and transmitted through a handheld device, preventing delays in diagnosis (Jezierski, 2014).

As chronic diseases and other long-term health issues become more prevalent in society, IoT enables an extension of mobile health (m-health) known as mIoT. In fact, Frost and Sullivan identified "health informatics" as one of the top ten medical device and information trends in 2015 (Frost 2015). Through mIoT, the healthcare industry is poised to offer assistance to those with chronic health conditions through wearable devices. A best case use of mIoT may be to monitor conditions such as diabetes, where constant streaming data on blood glucose levels are necessary for medical intervention (Istepanian, 2011). Accelerometers and other motion-based sensors can be used to capture the movement and vital signs of patients who have a condition – for example Parkinson's - that puts them at risk of injury. As just one

Figure 5.6: Typhoid incidence and human mobility from highly infected areas in Uganda during the January-May 2015 typhoid outbreak



Source: UN Global Pulse (2015).

example, the MyLively device allows family members to monitor the well-being of a relative in their home through strategically placed and wearable sensors that transmit motion data from within the home (MyLively.com, 2015). Wearable devices and non-invasive sensors will allow patients to lead more regular lives while providing ongoing data to doctors and hospitals.

IoT for climate change and disaster management

Today's array of sensors offered by the IoT paradigm also hold great promise for monitoring the effects of climate change, as IoT can leverage data from everything ranging from common devices – e.g. smartphones to take pictures, air quality monitors for detecting certain particulates, etc. – to large-scale devices – e.g. surveillance systems observing vegetative health, weather- and climate-monitoring devices, energy-managing systems (Box 5.4). These approaches and the successful use of their associated methodologies offer numerous opportunities for improving the effectiveness of humanitarian assistance and disaster relief (HADR) operations following natural hazards. Given the high value-added proposition of IoT in syndromic surveillance, many post-disaster response plans now include and emphasize the proviso that any damaged infrastructure (e.g. mobile cellular network) is to be repaired as quickly as possible so as not to impair IoT-based HADR efforts.

Small island developing States (SIDS) are particularly vulnerable to the effects of climate change, often owing to their remote locations and limited resources. This requires increasing self-reliance to anticipate the drastic effects to local economies, trade and tourism, food production and the health of the population, all due to rising sea levels, dramatic changes in weather patterns and global warming. It is important to

Box 5.4: IoT-enabled management of photovoltaic (PV) systems

Nest Labs is a ZigBee-based IoT company featuring three consumer home products: a thermostat, a smoke/carbon monoxide detector and a video camera. The main product, the Nest Learning Thermostat, is designed to learn and adapt to the user's schedule. After an initial 12-day acclimatization period, the thermostat adjusts the temperature in the home to more efficient heating and cooling based on patterns of life. The company was acquired by Google in 2014 for USD 3.2 billion dollars, and it has since made strategic partnerships in the renewable energy sector and the insurance industry (Higganbotham, 2015).

In early 2015, Nest partnered with SolarCity, a United States-based photovoltaic (PV) system company, to provide a limited number of free thermostats to customers. Unlike a smart meter, the thermostat will have more finely-tuned user data as more IoT-powered devices are connected to it, thereby allowing it to heat or cool each room individually, or having a trigger to initiate the change, for example starting a car at work. With many smart devices attached, it will be possible to establish precise energy-usage profiles and respond to peak demand by limiting the activities of other smart home devices (Baraniuk, 2015; Tilley, 2015).

With regard to inclement weather, sudden cloud cover would interrupt PV energy production and create a surge in demand for power from the grid. To prevent this potential generation rejection and circumvent a potential brownout or blackout, Nest could potentially communicate with household smart devices to reduce, pause or stop heavy power-consuming activities.

Previously, SolarCity, which also uses Zigbee in their PV array installations, created the MySolarCity App that captured generation and usage data in order to mitigate the issues that prevent solar energy from being more freely integrated into the grid. Where previously an audit conducted in the home as part of the installation process would have to manually add and account for energy usage of home electronics and heating, ventilating, and air conditioning, the Nest acts as an extensible hub within the IoT realm (Korosec 2015).

note that more than 50 per cent of Caribbean and Pacific island populations live within 1.5 km of the shore (UNESCO, 2014). In addition, special attention is being given to unsustainable practices and geological incidences, which can worsen or accelerate the effects of climate change.

The negative effect of climate change, as manifested in the increasing incidence of extreme weather events, poses a significant threat to the stable operation of a host of critical infrastructure systems, including transportation, energy delivery and telecommunications (Power, 2015). In particular, extreme weather events have the potential to compromise major communication backbones, such as the Internet, which rely largely on fixed data connections and power supplies (Hauke, 2014). In turn, a variety of IoT sensors and communication devices that use small amounts of battery power and transmit data through wireless communication protocols — independent of the Internet — can help to facilitate the operation of essential services and emergency management despite the loss of backbone communication infrastructure during large-scale natural disasters (Hauke, 2014).

In another example, sea-level rise, extreme storm intensification and other alarming trends increasingly threaten modern civilization along shorelines, which, historically, have represented the areas of high population growth. A wealth of sensors offered by the IoT paradigm can provide critical monitoring. As the cost and size of sensor devices decrease, their widespread deployment becomes an increasingly practical method for improving the ability to observe effects of climate change through crowd-sourced meteorological observation. By way of example, the Japanese firm Weathernews is distributing thousands of palm-sized atmospheric sensors to citizens, enabling them to measure and communicate temperature, humidity and pressure readings in real time, thereby increasing the granularity of weather forecasting and awareness of climatological phenomena (Hornyak, 2015). More granular atmospheric data can help to manage the impact of extreme weather events, as well as provide a richer body of evidence to inform computational models and drive more accurate analysis of patterns in global climate change (Faghmous, 2014). In the context of disaster scenarios, the prevalence of crowd-sourced radiation mapping efforts following the 2011 tsunami and Fukushima nuclear incident further demonstrates the speed with which impromptu sensing networks can be established (Plantin, 2015).

Aside from disaster scenarios, sensor networks can also be used for the research and monitoring of the environment, and to provide data about those parts of the planet still relatively unknown (Box 5.5). On a much smaller scale, the use of IoT in experiments, such as the Birmingham Urban Climate Laboratory's enhancements to the Road Weather Information System (RWIS), demonstrates that acquiring robust data on real-time road conditions can improve the maintenance of transportation infrastructure by precisely identifying which sections of roadway are most in need of repair or maintenance at a specific time (Chapman, 2014). Similarly, the "Padova Smart City" proof-of-concept project demonstrates a viable IoT architecture for fielding sensors to monitor the status of public infrastructure, such as streetlamps.

IoT for precision agriculture

The growing number of people in the world and the encroachment of megacities upon limited land resources, as well as increasing demand for food, beget a need for precision agriculture, which is ''that kind of agriculture that increases the number of (correct) decisions per unit area of land per unit time with associated net benefits.'' (McBratney, 2005). Although precision agriculture has been practised for several decades with the help of remote sensing by satellites (Mulla, 2013), the ability to integrate diverse data from an array of affordable sensing devices is a recent development that will enable a larger segment of the agribusiness community to leverage the advantages of technology.

Precision agriculture requires a large amount of connectivity, bandwidth and capable sensors in order to deliver timely and accurate data, which are the foundation for any precision agriculturalist's decision-making. IoT sensors and communication devices could be central to a number of precision agriculture processes, such as preparing soil, planting and harvesting at precisely the optimal time, thus ultimately helping to meet the challenge of increasing food production by 70 per cent by 2050 (Beecham, 2014).

Box 5.5: Monitoring the world's deep oceans

The negative effects of climate change are compounded by a relative paucity of sea-state data, and sparse ocean data acquisition endeavours. The tragic 2014 loss of Malaysia Airlines Flight 370 (MH370) reveals how little is actually known about the world's deep oceans, as an over-a-year-long search of more than 4 million square kilometres has turned up almost no trace of the aircraft or its 239 passengers (only a flaperon of the plane was found in Réunion in July 2015).[12] The global response has led international governing bodies to revise standards and practices for the civil aviation industry. ITU, having the mandate to coordinate global orbital resources and radio spectrum, was asked by the International Civil Aviation Organization (ICAO) to expand satellite capabilities for global flight tracking. As an outcome of ITU plenipotentiary conference Resolution 185, global flight tracking was added to the agenda of the World Radiocommunication Conference 2015 (WRC-15) (ITU, 2014c). In addition, ITU established the Focus Group on Aviation Applications of Cloud Computing for Flight Data Monitoring to determine the telecommunication standards needed for real-time monitoring of flight data.[13]

The case of MH370 lends credibility to the argument that we have greater knowledge of the surface of Mars and the Earth's Moon than we do of the topography of our own planet's deep oceans (Smith, 2014). Although ocean data acquisition systems (e.g. data buoys) have been in use for decades and have played a critical role in facilitating our knowledge of complex climatic phenomena, such as El Niño and El Niño Southern Oscillation (ENSO) (McPhaden, 1998), the advent of IoT represents an opportunity to significantly increase the value of data buoys and scientific understanding of the ocean. This potential is illustrated by the deployment, by the National Oceanic and Atmospheric Administration (NOAA), of the Chesapeake Bay Interpretive Buoy System, which collects and relays a variety of sea-state data in real-time for a host of applications, ranging from public education and weather monitoring to fisheries management and environmental protection (Wilson, 2011).

With the development of self-sustaining power sources such as microbial fuel cells (Tender, 2008) (a bio-electrochemical device that harnesses the power of respiring microbes to convert organic substrates directly into electrical energy) and wave energy harvesting (Hangil, 2014), it will be increasing affordable to deploy large fleets of drifting and moored buoys that improve our ability to monitor the ocean, understand its role in climate change, and prepare for potential disaster events emanating from the ocean. Another initiative to collect data from the oceans is the ITU/WMO/UNESCO-IOC Joint Task Force that investigates the use of submarine telecommunication cables for ocean and climate monitoring and disaster warning.[14]

By way of example, the successful implementation of a precision agriculture management system (PAMS) in Huaihua, Hunan, China, demonstrates that such IoT-enabled processes can maximize workforce productivity, while increasing and improving crop yields (Ye, 2013).

On the African continent, African farmers could indeed rise to this challenge if they had access to the requisite infrastructure and associated analytics. Raising productivity in agriculture is vital to transformative growth, and Africa's USD 35 billion food market (Munang, 2015) could well be served directly by its own farmers, if the aforementioned enhanced productivity paradigm existed.

As climate change shifts ecosystems and precipitation patterns, it will be necessary for farmers to adapt. The 2014 Big Data Climate Challenge winner from the International Center for Tropical Agriculture, Colombia, created an app-based tool for site-specific agriculture. The app combines multiple datasets to create recommendations for rice farmers who provide their individual data (UN Global Pulse, 2014)

The criticality of precision agriculture becomes particularly evident when analysing the trends of

developing countries, for as developing countries mature, most economic activities (e.g. agriculture, energy, industry, etc.) affect not only the quantity but also the quality of water resources, thereby further limiting acceptable potable water availability. Allocation of limited potable water resources among competing economic sectors will be an increasing challenge for many developing countries (Tilman, 2002), and failure to establish appropriate allocation mechanisms might impede further development, economic viability and latent stability (Gleick, 1993); if not properly addressed, exacerbated environmental pressures and social instability (e.g. increased income inequality) may result.

Precision agriculture techniques can be used to increase crop yield to keep up with demand. To ensure maximum crop yields, water supplies need to be predictable and timely. Predicting water supplies at a given time require "hyper-local" weather forecasting.[15] (Wakefield, 2013). One such example is IBM's Deep Thunder project, which focuses on generating hyper-local weather forecasts to gain more specific knowledge about weather, and translate this knowledge into insights for improved agricultural practices (Sonka, 2014). Capabilities, such as those offered by Deep Thunder, can help to inform a variety of farming decisions — from which seeds to plant and when to plant them, to when the use of fertilizers and pesticides should be avoided to prevent run-off and pollution (Jacob, 2014).

Certain technologies and other complementary offerings, comprising a highly effective architectural stack, are needed for the type of weather forecasting required by a precision agriculture paradigm. Sensors that allow for monitoring of crop growth rates, potential blight, water consumption, etc., will be required. These sensors will need to be connected to data collection systems. New platforms have emerged, such as unmanned aerial vehicles (UAVs), which can be used to collect the requisite information in rural areas and in the agricultural fields.

The use of drones accounts for as much as 90 per cent of seeding and pesticide spraying in Japan's agricultural sector (National Research Council, 2014) and provides an informative use case for how IoT-enabled devices can improve agricultural productivity. Whereas conventional aerial seeding and pesticide spraying by manned aircraft is both costly and imprecise due to the altitude from which such aircraft must deliver their payloads, unmanned aircraft are capable of delivering precise amounts of seed, fertilizer or pesticide to the exact locations in which they are needed (Huang, 2013). This allows farmers to maximize productivity by conserving seed and pesticide resources, while minimizing fuel and other aircraft operational costs. Unmanned aircraft are also capable of monitoring crop growth with greater efficiency than could be achieved with manned aircraft, satellite or other means, thus enabling farmers to accurately plan harvest schedules and identify particular areas in need of remedial pest control (Huang, 2013). By way of example, Field Touch is a service being piloted on 100 farms around Hokkaido, Japan, whereby data collected by unmanned aircraft are synthesized with other remote sensing data captured by satellite and weather monitoring devices in order to generate recommended courses of action for individual farmers (Kiyoshi, 2014).

IoT to address key challenges faced by megacities

Many people are moving to urban areas and cities, leading to the development of a growing number of megacities. According to United Nations statistics, currently 54 per cent of the world's population live in urban areas, and by 2050 that figure is expected to grow to 66 per cent (United Nations, 2014). Indeed, urban areas and city centres of the world are exploding, and the number of megacities, usually referring to an urban area with over 10 million inhabitants, is increasing rapidly. As at 2015, there are 34 megacities in existence compared with only ten in 1990 (United Nations, 2014). The urban sprawl - the predominantly unplanned, uncontrolled spreading of urban development into adjacent areas at the edge of the city- often means that existing critical infrastructure is not designed to accommodate the high capacities required by such rapidly burgeoning resident populations. The rise of megacities has led to overstressed infrastructures and unreliable delivery mechanisms, and presents a host of development challenges. These include the provision of adequate basic public infrastructure services, including sustainable, reliable and efficient energy, potable water and adequate sewage disposal and sanitation.

Growing cities are creating massive use of IoT applications and demand for smarter grids to maximize efficiency from energy sources while enhancing the stability of the grid, smarter water use from an ever-diminishing water supply, and more connectivity for better situational awareness and a better sense-and-respond paradigm. To best illuminate the interconnections and various demands for energy, water, sewage disposal/ sanitation and transportation, it is useful look at electrical utilities, water resource authorities, waste management authorities and transportation authorities and how they are taking advantage of IoT for converting megacities into smart cities (Box 5.6).

One example is the city of Sao Paulo, Brazil, which is home to the world's most complex public bus transportation system, transporting over 10 million passengers per day on over 26 000 buses (Guizzo, 2007). IoT helps such a large bus rapid transit (BRT) system operate effectively, by tracking the movement of buses via GPS, synchronizing traffic signals, enabling electronic payment to streamline boarding processes, and disseminating real-time route progress to assist travelers in their trip planning (Hidalgo, 2014). The city of Rio de Janeiro's Centro De Operacoes Prefeitura Do Rio is a nerve centre for the city, combining data feeds from 30 agencies, including transportation, utilities, emergency services, weather and other information submitted by city employees and the public via phone, Internet and radio, all in order to synchronize the delivery of essential public services (Kitchin, 2014). Integrating diverse data from across various systems operating in a single municipality in order to achieve more complete situational awareness and efficient operations is a primary tenet of the smart city paradigm (Gaur, 2015). The city of Songdo, Republic of Korea, embodies such a concept, as it is built to be smart from the ground up, with each residence and office networked through a centralized monitoring infrastructure, including an automated refuse collection system that sucks garbage through chutes from all around the city into treatment centres that will ultimately transform the waste into a sustainable power supply (Marr, 2015).

Box 5.6: IoT as an enabler of smart cities

Although there is no universally accepted definition or set of standards for what constitutes a smart city, all smart city initiatives are characterized by the pervasive employment of technology intended to make better use of a city's resources (Neirotti, 2014). In particular, IoT plays an important role in a city becoming smart, as evidenced by the case of Singapore. Singapore is unique in that it is a city-State. As a nation, it has recently unveiled a bold Smart Singapore strategy, which aims to convert the city-State into the first true smart nation through a range of initiatives leveraging intelligence, integration and innovation to become a major player on the world stage. Part of this strategy involves the implementation of heterogeneous networks that will allow mobile users to transition smoothly between wireless networks, as well as a roll-out of smart aggregation gateway boxes containing sensors, connected via fibre optic cables, which will collect and deliver real-time information to government agencies and citizens.[16] (Hidalgo, 2014).

In contrast, Shanghai's development as a smart city is conceptualized around the five "I"s of: (1) Information Infrastructure focusing on broadband access and wireless connectivity;(2, 3) Information Perception and Intelligent Applications focusing on governance and livelihood issues; (4) New Generation of Information Technology Industry focusing on urban self-sensing, self-adaptation and self-optimization; and (5) Information Security Assurance (Lin, 2015).

The rise of IoT offers developing nations the potential to segue from stressed megacities to smarter cities by converging various IoT-centric lines of effort towards the overarching strategic goal of a "smart city" paradigm. These IoT-centric efforts might relate to precision agriculture for the production of food, monitoring for water quantity as well as water quality, and observing for indicators that might impact the normal operations of the electric grid and other elements of critical infrastructure.

Electric grids, water and sanitation management

The Institute of Electrical and Electronics Engineers (IEEE) defines a smart grid as "an electric system that uses information, two-way, cyber-secure communication technologies, and computational intelligence in an integrated fashion across the entire spectrum of the energy system from the generation to the end points of consumption of the electricity" (Ghafurian, 2011).

Electrical utilities employ networks of sensors that can monitor the flow of electricity to better ascertain fault location and other related failures more quickly. In particular, the use of phasor measurement units (PMUs) has given rise to wide-area monitoring systems, in which the generation, transmission and distribution of electricity can be measured in near-real time (Ghosh, 2014). Although electric grid systems operate at a rate of many cycles per second (60 cycles per second in the United States, 50 cycles per second in the United Kingdom), conventional monitoring systems such as supervisory control and data acquisition (SCADA) are only capable of recording one measurement every two to four seconds (Sharma, 2014). In contrast, PMUs can record multiple measurements in a single cycle and communicate these data to centralized data concentrators, enabling system operators to gain a much clearer picture of the complex dynamics at play throughout electric grids (Aminifar, 2014).

By way of example, on 30 and 31 July 2012, the Indian electric grid suffered a series of cascading failures due to oscillations and load imbalances among three of its five interconnected grids that resulted in the largest blackout in world history, with over 620 million citizens left without power (Lai, 2012). A more robust monitoring capability, including PMUs, could have prevented the 2012 blackout (Pal, 2014), and the power grids of the Indian operators have begun deploying PMU or synchrophasor capabilities in order to enhance the system's reliability and move towards a smarter grid (Saha, 2015). Indeed, synchrophasors, smart meters and other IoT-enabled capabilities are central to the achievement of smart grids that can quickly assimilate diverse data and take corrective action in order to maintain stable power supplies (Moslehi, 2010). In India, the deployment of IoT-enabled synchrophasors has facilitated the consolidation of five previously interlinked grids into a single national grid, as well as the continually increasing incorporation of renewable energy sources (Mukhopadhyay, 2014).

Likewise, water resource authorities utilize networks of sensors for continually monitoring water quality and water supply security. In parallel, waste management authorities utilize sewage sensors to assist in the various efforts to monitor public health. Sewage sensors have even been used to monitor for other elements, including drugs, bombs, etc., that represent a danger to the community at large (Heil, 2012).

Just as the ability to acquire precise measurements regarding electricity is central to a smart grid, the ability to acquire precise measurements regarding water quality is central to smart water management. By way of example, the use of quick deployment sensor networks (QDSNs) in Valencia, Spain, is enabling system operators to monitor various aspects of water quality throughout the city's network of sanitary sewers in order to quickly identify malfunctioning components in the water management cycle (Bielsa, 2012). Such an IoT capability is especially valuable during periods of heavy rain or other extreme weather, when water management systems are under heightened stress.

Infrastructure and traffic control

Rapidly distending cities are accompanied by a rising number of cars and other forms of transportation, forcing policy-makers to look into better ways of monitoring and managing traffic. Next-generation sensor networks can assist in realizing more effective traffic flows for all modes of transport, identify shortcomings in infrastructure and help reduce CO_2 emissions. Indeed, WSNs are also being used for smarter transportation. For example, traffic lights are equipped with countdown timers and electronic signs that display various speed limits depending upon the information they collect from optical and/or radar-based sensors that provide information regarding the occupancy of individual lanes and/or the speed of vehicles. Upgrading the infrastructure of an existing intersection with state-of-the-art technology requires also providing the necessary communication links between all these components. Wireless technology can help reduce the cost by eliminating the need to route communication cables (e.g. Ethernet) to all devices

in an intersection. As WSNs, which are deemed to be a revolutionary information-gathering method, are increasingly becoming a critical part of the ICT infrastructure that underpins the reliability and efficiency of infrastructure systems, they are becoming the key technology for IoT.

IoT projects to monitor and improve transportation systems include:

- The New York City's Transportation Alternative's "CrashStat" (Lovasi, 2013), which uses reports of "near miss" accidents to identify high-risk traffic trouble-spots;
- the City of Boston's Office of New Urban Mechanic's mobile application "Street Bump" (Harford, 2014), which uses a phone's accelerometer to detect potholes while the application user is driving around the city; and
- the "Crowdsourcing Urban Simulation Platform" (Shin, 2011), which uses the phone's accelerometer and location data to deduce the mode of transportation. Further, the platform uses location and time stamp data (i.e. correlated against pattern of life data) and attempts to recognize the current activity (e.g., whether one is at work, home, etc.). By using the vehicle type and location activity, the framework endeavours to compute urban sustainability values, such as what amounts of CO2 emissions are generated, and examines how well the city was, is and can be for the commuting requirements of its residents.

At the same time, an increasing amount of research is focusing on the safety and needs of cyclists and pedestrian access, particularly as more cities around the world promote citizen health and a "green community" (Bichard, 2015). For example, IoT is being used to help cyclists identify better routes to choose, as illustrated by the MIT Media Laboratory's Mindrider project (Box 5.7).

Natural hazards

Megacities, particularly those along shorelines, are burgeoning, and these population centres tend to be particularly susceptible to the effects of land erosion, hurricanes, flooding, salinization issues, major land subsidence, etc.

Robust sensor networks are highly capable of providing some semblance of early warning for punctuating events and can continuously monitor changing conditions, which may be indicators of risk. The hitherto acceptable paradigm of static data and batch processing may no longer be viable in this data environment, wherein streaming data and in-stream processing of continuous data streams become vital for these densely populated areas. This migration from static to streaming data is exemplified by the implementation of smart grids. Whereas conventional equipment used for monitoring fault or disturbance events in an electric grid have been event-driven (i.e. they only began recording once a disturbance event had occurred), synchrophasors and other wide-area-measurement capabilities constantly record

Box 5.7: Mindrider

Mindrider is a project born and spun out of the MIT Media Laboratory. The project features a helmet with: (1) a forehead-based sensor that uses electroencephalography (EEG) to measure electrical activity (i.e. brainwaves) in a bicycle rider's brain (Davies, 2015), and (2) an ear-based sensor that helps to remove noise from the EEG signal (Walmink & Wilde, 2014). The MindRider helmet also features a light-emitting diode (LED) that glows green to indicate a "calm state of mind" or red for a "more stressed state of mind" during a cyclist's journey. The MindRider helmet is Bluetooth compatible, and the information from the EEG sensor can be fed into an application on the user's smartphone, which uses the onboard GPS to map the relaxing "sweetspots" in green and the stressful "hotspots" in red (Walmink & Chatham, 2014). In this way, other cyclists can note where the hotspots are and pay particular attention to the reasons behind them — whether they are high-traffic areas requiring extra caution or dangerous areas that should simply be avoided. For commuters, this could help in the evaluation of alternative routes and identification of better routes.

and transmit data regarding the system's state (Kezunovic, 2012).

Lack of adequate infrastructure and cyber vulnerabilities remain a challenge for IoT

As highlighted in the previous section, there is great potential for IoT to help address some of the world's most pressing development challenges. At the same time, the deployment of IoT applications and their effectiveness depend on the availability, quality and safety of the underlying network. Although some of the IoT applications can be used over low-bandwidth networks (see Box 5.8), many monitoring efforts require significant amounts of bandwidth. Moreover, even IoT applications requiring low bandwidth may demand a high-capacity infrastructure if they are to be deployed in dense areas where other IoT/ICT applications are running concurrently. There is therefore a risk that countries and communities that do not have access to high-capacity ICT infrastructure are left behind IoT.

At the same time, the quantity and quality of networks differ markedly between countries, cities and regions and in particular between urban and rural areas. Internet connectivity is not yet available to all parts of the world and there are increasing efforts to bring Internet connectivity to currently unconnected and remote areas. Although urban centres are home to 54 per cent of the global population and are, appropriately, a major focus of infrastructure improvement and protection, the importance of Internet connectivity for rural and physically isolated areas should not be overlooked.

In expanding access to the Internet, there needs to be a careful counterpoising between reach, performance and cost. As Internet connectivity increases and a variety of actors endeavour to expand global Internet accessibility, the underlying ICT infrastructure remains somewhat brittle in key technological areas.[17] The cost of expanding fixed infrastructure to remote and isolated areas is often prohibitively expensive. Mobile broadband can contribute to covering the gap, and satellite broadband (Boxes 5.9 and 5.10) is the technology most commonly employed in making broadband access universal. Taking account of the progress made in satellite technology, some of the past restrictions on the use of satellite connectivity for IoT deployments have disappeared, although cost and performance requirements still need to be carefully considered in each specific IoT implementation. Mobile infrastructure provides an intermediate solution between the cost and capacity of fixed broadband and those of satellite-broadband networks. However, mobile networks ultimately depend on good fixed connectivity in the backhaul and backbone of the network if the capacity requirements increase. In an IoT scenario, more capacity will be required either because there are more IoT applications running concurrently on the network or because the IoT applications are upgraded and become more bandwidth-hungry.

Box 5.8: Second generation (2G) networks and IoT

The number of M2M subscriptions in developing countries overtook those in developed countries by the end of 2013 according to GSMA Intelligence (GSMA, 2014c). Mobile wireless communication platforms can support data collection and transmission through a variety of applications, such as EpiCollect, Magpi and ODKCollect, which can in turn be implemented for many process-automation and remote-sensing functions (Baumüller, 2013). Indeed, even technology as basic as second-generation (2G) wireless networks may be able to serve as gateways into IoT functionality (Zhu, 2010). In rural communities with limited access to either fixed or wireless broadband, finding inventive ways to leverage the advantages of networked sensors is especially valuable (Sivabalan, 2013). By way of example, GPS-equipped mobile devices affixed to livestock are assisting with tracking stolen cattle in Kenya, while data from weather stations trigger micro-insurance pay-outs by mobile phone in the event of extreme weather and herd loss (Baumüller, 2013). In addition, organizations like the Syngenta Foundation have been working to develop applications that leverage mobile wireless M2M to increase efficiency in agricultural processes and track the supply of agricultural products (Brugger, 2011).

Box 5.9: Geosynchronous satellites

Communication satellites and weather satellites often utilize geostationary orbits (GEOs). In this scenario, a satellite orbits the Earth along a circular path 36 000 km above the Earth's equator at 0° latitude, following the direction of the Earth's rotation and proceeding at the same speed as the planet is turning, thereby enabling the satellite to stay in place over a single location. Owing to the constant 0° latitude and the nature of geostationary orbits, the location of satellites in GEO differs by longitude only. Compared to ground-based communications, all GEO satellite communications experience higher latency due to the signal having to actually travel the 36 000 km to the GEO satellite and back to Earth again. This delay can be significant (about 250 milliseconds to travel to the satellite and back to the ground) even though the signal is traveling at the speed of light (about 300 000 km per second). This latency may be somewhat mitigated for Internet communications with TCP features that shorten the round trip time (RTT) per packet by splitting the feedback loop between the sender and the receiver.

Box 5.10:Low Earth orbit (LEO) and medium Earth orbit (MEO) satellites

A low Earth orbit (LEO) is an orbit around the Earth at an altitude of between 150 and 2 000 km A medium Earth orbit (MEO), also known as an intermediate circular orbit (ICO), is an orbit around the Earth at an altitude of between 2 000 and 36 000 km. These lower orbits (as compared to geostationary orbits) may cause LEO satellites to be visible from Earth for only an hour or less before they go over the horizon and out of range. Unlike GEO satellites, LEO satellites do not appear at a fixed position in the sky. In order for the ground-based antennas that communicate with these satellites to be as simple as possible, a constellation of LEO satellites is required, with relaying and passing-off of information from one satellite to another so as to hand over the fixed-position terrestrial signal.

Apart from the underlying infrastructure, the success of IoT also depends on the resilience and safety of the network, services and applications. Despite the positive benefits and attributes, it is necessary to be aware both of the technological efforts needed to mitigate against cyber vulnerabilities plaguing the aforementioned sensor networks, and of malicious acts by people, including acts of vandalism, sabotage or even terrorism. These can have significant negative impacts on the development and reliability of IoT applications. Something as simple as a vandalized traffic signal can cause very serious hazards to traffic flow as well as to pedestrians. Other simple acts of vandalism (e.g. destroying a fire hydrant), while not directly life-threatening, can be significantly wasteful of all the efforts that went into sourcing, treating and managing the water supply to improve the availability of potable water. It is easy to see that some elements of the current infrastructure that might have been considered non-critical are in fact critical nodes in a highly connected world.

5.4 Conclusions and recommendations

Several ICT developments are accelerating the progress of IoT: low-cost and low-power sensor technology, growth in high-speed and high-quality infrastructure, near ubiquitous wireless connectivity, an increase in the number of devices with embedded communication capabilities, large amounts of available and affordable (predominantly cloud-based) storage space and computing power, and a plethora of Internet addresses from the advent of the IPv6 protocol.[18] The high expectations that IoT is generating in many sectors – e.g. education, healthcare, agriculture, transportation, utilities and manufacturing – are encouraging more stakeholders to enter the market, thus contributing to its expansion.

Because it is cross-cutting, IoT can significantly contribute to the achievement of development

goals that go beyond the ICT sector, including those addressed by the new Sustainable Development Agenda. For instance, IoT is poised to become a building block of tomorrow's sustainable cities and communities, as well as a key element in future climate action, clean water sanitation systems and the renewable energy value chains. This chapter has presented a number of concrete examples of how innovative IoT services and applications are already being used to deliver better healthcare services, address key challenges of climate change and disaster management, and contribute to precision agriculture. IoT is also a key driver in the approach to make cities smarter and help governments deliver better basic services.

However, IoT opportunities are not equally distributed between and within countries, and in order to unlock the potential of IoT as a development enabler, several challenges remain to be addressed, both within and outside the ICT sector.

IoT brings together and requires the cooperation of various stakeholders in the ICT sector: from consumer electronics manufacturers to telecommunication service providers and application developers. In addition, for IoT to fulfil the high expectations created, other stakeholders outside the ICT sector need to be engaged, including car manufacturers, utilities, home-appliance manufacturers, public administrations and many others. Bringing together all these stakeholders adds considerable complexity to the development of IoT, but it is a requirement to ensure interoperability, which is regarded as the key to unlocking as much as 40 to 60 per cent of IoT's potential value (McKinsey, 2015). This is a paramount challenge to be addressed in ITU and other forums.[19]

Most of the value derived from IoT comes from the generation, processing and analysis of new data and use of the insights extracted therefrom for specific decisions in each domain in which IoT can be applied. The value of IoT is therefore closely linked to the exploitation of big data, and thus the challenges in terms of data management are similar to those of other big data applications. In this regard, national statistical offices have an important role to play given their legal mandate to set the statistical standards, and they could for instance become standards bodies and big data clearing houses that promote analytical best practices and facilitate data sharing (ITU, 2014b). National telecommunication regulatory authorities have a complementary role to play, considering that most IoT data are transferred through telecommunication networks. Indeed, regulators could facilitate the establishment of mechanisms to protect privacy and foster competition and openness in data markets (ITU, 2014a). In this regard, public administrations could also contribute significantly by adopting open data policies for their IoT datasets.

Lastly, ICT infrastructure underpins the connectivity and data processing capacity required for IoT. Although wireless coverage is almost universal through satellite and mobile networks, the actual ICT connectivity required for unlocking the full potential of IoT may be more demanding. Indeed, some IoT applications may run with low-speed, low-capacity connectivity, but others will require high-capacity broadband connections. Even in a scenario with IoT applications requiring low capacity, the simultaneous use of numerous devices may make a high-capacity backhaul or backbone connection necessary. In addition, the processing of big data generated by IoT will require bandwidth. This applies even more in areas with limited IT infrastructure, where the storing and analytical capabilities will be in the cloud and rely on high-capacity transmissions. Fixed-broadband connectivity is the most suited to meet these requirements, along with sufficient international Internet bandwidth and backbone capacity. Data presented in Chapter 2 show that fixed-broadband uptake in the developing world remains very limited and that there is a scarcity of international connectivity in many developing countries. This holds particularly true for the least connected countries (LCCs) and suggests that LCCs do not have the necessary ICT infrastructure for IoT, despite being those countries that could benefit the most from its potential for development. This calls for additional policy and regulatory action to close the fixed ICT infrastructure gap in the developing world and avoid many developing countries being left behind in the IoT race.

Endnotes

1 Recommendation ITU-T Y.2060, available at: https://www.itu.int/rec/T-REC-Y.2060-201206-I.

2 Cox, Landon. "IoT Vs M2M: Understanding the Difference." PubNub, 2 January 2015. Available at:http://www.pubnub.com/blog/iot-vs-m2m-understanding-difference/.

3 Z-Wave is a wireless technology designed to allow regular household devices to communicate among themselves and to be accessed and controlled remotely. For more information, see: http://www.z-wave.com/what_is_z-wave.

4 Macmanus, Richard. *Chinese Premier Talks up Internet of Things.* Readwrite2010. Available at: http://readwrite.com/2010/01/19/chinese_premier_internet_of_things.

5 McLellan, Charles. *The Internet of Things and Big Data: Unlocking the Power*. ZDNet Review, March 2, 2015.

6 Ibid.

7 Ibid.

8 Gartner. "Gartner Says the Internet of Things Will Transform the Data Center. Gartner, Inc, 2014. Available at: http://www.gartner.com/newsroom/id/2684915.

9 Woollaston, Victoria. *Revealed: What Happens on the Internet in Just One Minute*. Daily Mail, 30 July 2013.

10 Google Official Blog, *We Knew the Web was Big…* Google, Inc. 25 July 2008. Available at: http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html.

11 Open Education Database. *The Ultimate Guide to the Invisible Web*. 11 November 2013. Available at: http://oedb.org/ilibrarian/invisible-web/.

12 See http://www.mh370.gov.my/phocadownload/News/FLIGHT%20MH370%20ARTICLES%20200815.pdf.

13 For more information on the Focus Group on Aviation Applications of Cloud Computing for Flight Data Monitoring, see: http://www.itu.int/en/ITU-T/focusgroups/ac/Pages/default.aspx.

14 For more information on the ITU/WMO/UNESCO-IOC Joint Task Force, see: http://www.itu.int/en/ITU-T/climatechange/task-force-sc/Pages/default.aspx.

15 Wakefield, Jane. *Tomorrow's cities: How big data is changing the world*. BBC. Aug 28 (2013).

16 Information Communications Development Authority of Singapore. *Singapore Lays Groundwork to be World's First Smart Nation*. 18 June 2014. Available at: https://www.ida.gov.sg/blog/insg/featured/singapore-lays-groundwork-to-be-worlds-first-smart-nation/.

17 Singh, Pradeep Kumar, et al. *Autonomic computing: A revolutionary paradigm for implementing self-managing systems*. Recent Trends in Information Systems (ReTIS), 2011 International Conference on. IEEE (2011).

18 Plonka, David and Arthur Berger, *Temporal and Spatial Classification of Active Ipv6 Addresses.* arXiv preprint arXiv:1506.08134 (2015).

19 See for example the standardization work of ITU-T Study Group 20 on IoT and its applications including smart cities and communities.