DOI: 10.15199/13.2016.10.18

The Internet of Things – from smart packaging to a world of smart objects?

(Od inteligentnych gadżetów do świata inteligentnych obiektów)

prof. dr inż. WOJCIECH NOWAKOWSKI, Instytut Maszyn Matematycznych, Warszawa

Abstract

Due the growth of internet network are formed ideas, to enlarge the "intelligence" of objects (for example sensors), so that they can by internet to communicate with a man or a computer...

Keywords: Internet of Things, Intelligent world, New Internet

Streszczenie

W związku z rozwojem sieci internetu powstały pomysły, by tak powiększyć „inteligencję" przedmiotów (np. czujników), aby mogły one za pomocą sieci porozumiewać się z człowiekiem lub komputerem...

Słowa kluczowe: Internet of Things, IoT, inteligentny dom, inteligentny czujnik, nowe wcielenie internetu

The term "Internet of Things" was first used in 1999 by Kevin Ashton, a British technology pioneer and the co-founder of the Auto-ID Center at the Massachusetts Institute of Technology (MIT), which was set up to study RFID (Radio Frequency Identification). RFID is a generic name for technologies that use radio waves to automatically identify an object by means of a small electronic chip, the so-called tag. Originally Ashton became interested in the RFID tags – then being used for the first time in loyalty cards – merely as a replacement for the barcode, a part of "smart packaging" intended to facilitate the tracking of inventory of fast moving consumer goods in real time. However, one significant difference between the bar code system and the RFID tags was that the latter did not require a dedicated reader, as the data they contained could be transmitted wirelessly and read by any device; this, in turn, opened up a range of interesting possibilities, some of them far removed from inventory tracking.

It is the RFID tag – which can be attached to (or implanted into) almost anything, including living beings, turning it into a potential data transmitter – which provided the foundation for the idea of the "smart object". At first it was little more than an extension of "smart packaging" - the RFID tags were to be identifiers, allowing computers to manage and inventory all the things (and people) around them. Instant and constant inventory control was to become ubiquitous, and experts envisioned such implementations as, for instance, remotely enforcing copyright restrictions for digital works.

However, as technologies developed, new hardware platforms came into being, cheaper connectivity became available, and possible new applications were envisioned, this original concept was transformed and extended. The smart objects of today are much more advanced electronic devices containing a microprocessor and a communication unit, but also sensors and/or actu-

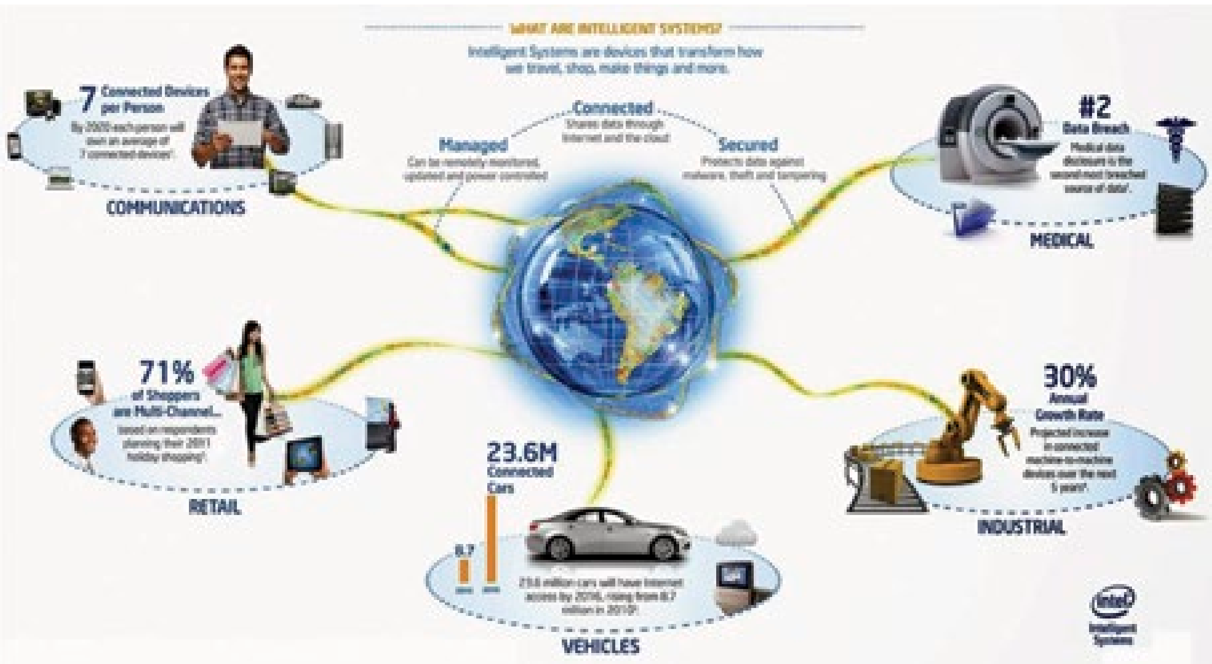

Fig. 1. The intelligent world as envisioned by the Intel Corporation. Rys. 1. Inteligentny świat w wizji firmy Intel

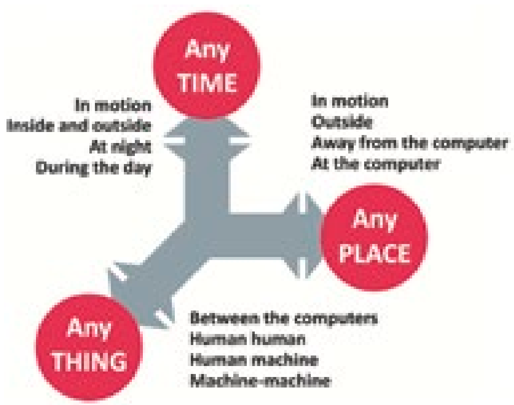

Fig. 2. The concept of the Internet of Things
Rys. 2. Ogólna koncepcja Internetu Rzeczy

ators [1]. To refer to them, the writer Bruce Sterling has even introduced a new, futuristic term *spime* defined as *an object of unique identification, aware of its location, its environment, that intitializes and auto-documents itself, and launches data about itself and its environment in large quantities*. In other words, the smart objects are not limited to storing digital information and transmitting it wirelessly on demand, but can also process and analyse data in order to make decisions, and even act on them (introducing changes in the world around them) using the actuator modules. They are not limited, either, to the information with which they were originally programmed – they can both send and receive data to and from other devices (and, by the same token, their human users) by means of internet protocol, and the sensors allow them to "feel" their environment, collecting information about their surroundings.

Smart objects can be embedded into almost any device, such as industrial equipment, home appliances, light switches, engines and many, many others. This, in turn, makes possible countless uses in industry, business, the household – in short, everywhere. Smart alarm clocks, for instance, could wake you up earlier if they receive information about unusually heavy traffic; sensors attached to plants will indicate the best time to water or fertilize them; smart running shoes would monitor the time, speed and distance for the purpose of ascertaining progress or even competing with another runner in any location on Earth, and the smart medicine container can signal that a medicine has not been taken at the proper time.

The Internet of Things is where the "smart objects" and the Internet come together (and indeed its alternative names is the Internet of Smart Objects).

It is envisioned as a huge network connecting almost all kinds of devices - from buildings, vehicles and other machines to daily necessities and all kinds of sensors – which goes beyond machine-to-machine (M2M) communications to link the two known worlds – of Things and of People, as all these devices are to be remotely accessible and controllable by means of the Internet. In other words, It is a vision in which the Internet extends into the real, physical world. Another interesting definition was provided by Ricardo Murer from the Internet of Things Council's think tank, who wrote that *the Internet of Things is an open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in their environment.*

The concept of the Internet of Things rests on three assumptions: anytime, anywhere and anything.

These, in turn, relate to the basic capabilities of smart objects:

– self-identification: each object has an unique identity and must be capable of transmitting information about itself.

– communication: each objects must be capable of communicating with other objects

– cooperation: all objects must be capable of influencing one another.

Below are the key characteristics of the Internet of Things, and some associated challenges:

Heterogeneity of devices. Among the huge number of connected devices there is a large variety with regard to their computational and communicative capacities. Support for the heterogeneity of the internet of Things must be provided by means of architecture and protocols to ensure seamless interoperability.

Scalability. As time passes, more and more devices of all kinds will enter the Internet as smart objects; the problem of scalability involves addressing and naming, two-way communication (that is, the number of connections between various elements of the network), the huge amount of data, managing information and the provision of appropriate services.

Ubiquitous data exchange by means of wireless technologies. Difficulties in meeting this requirement involve restrictions in radio frequency transmissions, as well as the issues of bit rate and latency.

Optimum energy solutions. One vital issue is the optimization of energy use considering the huge amounts of data being transmitted and the large number of dispersed devices.

Localization and location tracking. Any device that is part of the Internet of Things can be identified in one way or another. Therefore, it becomes possible to pinpoint its location, which opens up completely new possibilities for logistics and supply chain management.

Self-organizing capabilities. The complexity of the systems requires the provision of self-organization and self-configuration mechanisms to minimize human intervention.

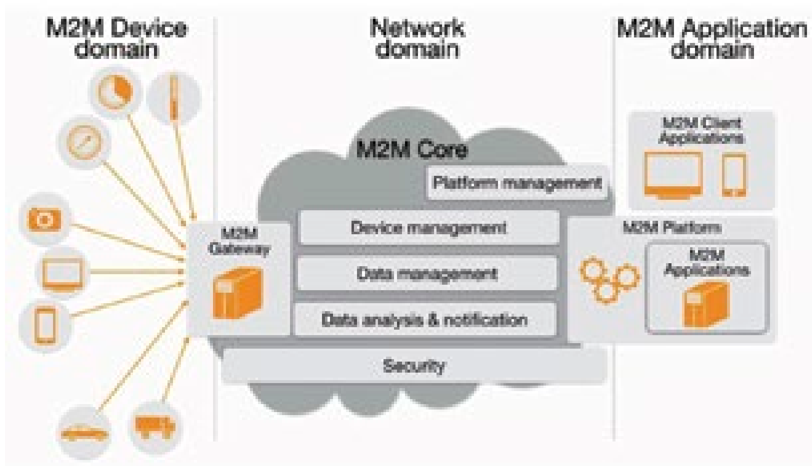

Fig. 3. M2M network scheme (http://dtpoland.com)
Rys. 3. Schemat sieci M2M (http://dtpoland.com)

Data management. The exchange and analysis of data is the core of the Internet of Things. Therefore it is necessary to use appropriate data models and semantic descriptions of their content, including the appropriate language and format.

In-built security and privacy protection. Due to close links with the real world, the technologies of the Internet of Things must offer the appropriate levels of security and privacy.

It is also important that the network architecture and technological solutions for the smart objects be flexible, for at present it is impossible to predict all the directions of future technological development. The older systems, usually optimized for specific applications and uses, are difficult to adapt to other scenarios, first and foremost because they lack the mechanisms for interoperability and integration with the new network mechanisms. To extend the Internet in such a way that it would become possible to connect practically any chosen device will require the creation of new communication standards, security and privacy mechanisms, a migration to the new IPv6 protocol and a decentralized structure for data management and the provision of services.

The IoT as a stage in the evolution of the Internet

Why is the Internet of Things so important? To answer this question we must first understand the difference between the Internet and the World Wide Web (www), two terms which are often used interchangeably:

– The Internet is the physical layer, the networking infrastructure, comprised of computers and other devices, such as switches and routers, which connect them and allow them to communicate. Its main function is the transmission of information – quick, reliable and secure – from one point to another. Information that travels over the Internet does so via a variety of languages known as protocols.

– The World Wide Web is the application layer, running on top of the physical network of the Internet. It is the system we use to access the information that is transmitted on the Internet.

The network of WWW applications has gone through a number of evolutionary stages.

In the first, research stage the Net – then called the Advanced Research Projects Agency Network (ARPANET) – was used largely for research purposes by members of academic institutions.

In the second stage the brochureware function was created, to allow the publication of information on the Internet, so that all users could learn about the products and services offered by various companies.

In the third stage transaction information was moved onto the network, so that products and services could be bought and sold online. It was then that the great Internet commerce companies such as, for instance, eBay, Amazon, or the Polish Allegro came into being.

In the fourth stage – in which we still are – the Internet became a platform for social networking. Companies such as Facebook, Twitter or Groupon became very popular and lucrative because they made it possible for everybody to share various multimedia information with their friends or relatives.

At present the Internet is used by more than two billion people all around the world, who visit webpages, receive and send e-mail messages, watch all sorts of multimedia content, play games, use the social media and all kinds of applications. The number of people with access to this global network will grow, and soon we are likely to witness a huge technological leap forward, which will make it possible for the Internet to become a global platform not just for people, but also for various machines, sensors and other smart objects which will be able to communicate with one another, exchange information, perform calculations and initiate all sorts of actions.

It has been forecast that the most rapidly increasing group of Internet "users" will be those objects, the work of human hands. It is estimated that within a decade 75% of the inhabitants of the world – that is, about 5 billion – will have Internet access, while the number of devices connected to the global network is to exceed 25 billion. And this rapid growth of the numbers of connected devices is already occurring, due to the spread of tablets and smartphones.

The Internet itself has entered a stable development path and is not changing significantly. It operates just as before, on the old IP protocol. However, its evolution into IoT will be a major developmental leap. Even today, thanks to intelligent sensors we can use the Internet network to transmit all sorts of information – such as temperature, pressure, vibration, light, humidity, and even stress – and react to it. Furthermore, the Internet is spreading into places that had been unreachable before. It has even found its way into space thanks to the IRIS (Internet Routing in Space) program. The evolution of the Internet into the Internet of Things will lead to the collection, storing, transmission, analysis and dissemination of data on a mass scale, which is likely to give rise to many new phenomena.

Since 2013 the vision of the Internet of Things has been changing due to the proliferation of many different technologies, from wireless communication to micro-electromechanical systems (MEMS) used in the traditional areas of control systems and automation, for instance in the household and construction. The literature on the subject considers as the world's first smart network device a Coca-Cola machine at Carnegie Mellon University, which was connected to the Net in 1982, allowing it to transmit information about the number of cans and their temperature. In 1994 the idea of a network of such devices was described as the movement of *small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories*. Between 1993 and 1996 some companies already began offering such solutions (Novell's *Nest* being one example). However, it was only in 1999 that the idea of the Internet of Things really took off, mostly through the Auto-ID Center at MIT and related market-analysis publications.

From the very start it was obvious that the IoT would consist of a huge number of devices connected to the net, which meant that all those devices would use an IP address as their unique identifier. The address space of IPv4 – the protocol currently in use – is limited (only about 4,3 billion of unique addresses). However, a new protocol, IPv6, has already been introduced, with a huge address capacity, and also some new features which, for instance, simplify the allocation of addresses and improve network management and routing efficiency. The use of this new protocol is of vital importance for the development of the IoT.

Are we there yet?

Although the term has already become something of a buzzword, it has to be said that the vision in its entirety is still far from being realized.

At present the "Internet of Things" is still a loose, dispersed collection of autonomic networks, each set up for specific purposes. For instance, in a car there are many internal networks: to manage the working of the engine, to ensure comfort or safety while driving, for navigation etc.

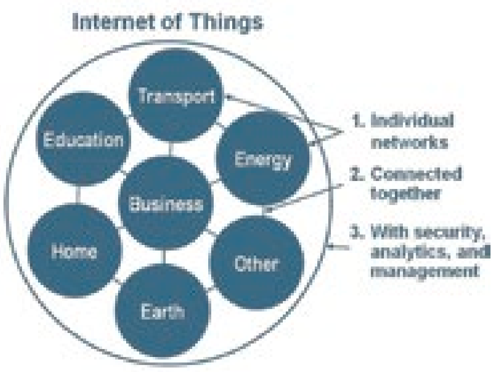

Fig. 4. Network of networks. Rys. 4. Internet jako sieć sieci

Commercial and residential buildings also employ various systems – for the management of heating, lighting, ventilation, internal conditioning (HVAC), telecommunication services, or security. For this reason Jan Holler of Ericsson has even dubbed the present state of affairs "a collection of Intranets of Things". Once the Internet of Things is fully implemented all these networks will be integrated and augmented with additional functions for the purposes of security as well as analytics and management.

How far along this road are we? It might be worth quoting an interesting claim about IoT formulated by Cisco's Internet Business Solutions Groups (IBSG), a leader in the field of IoT-related technologies: we can speak about the creation of the Internet of Things when the number of things (objects) connected to the internet will exceed the number of all the human beings on Earth. In 2003 our planet was inhabited by about 6,3 billion people. On the other hand, the estimated number of devices connected to the Internet at the time was about 500 million, that is, less than 8 for every 100 inhabitants of Earth. In 2015 we have already moved much further towards the threshold suggested by Cisco..

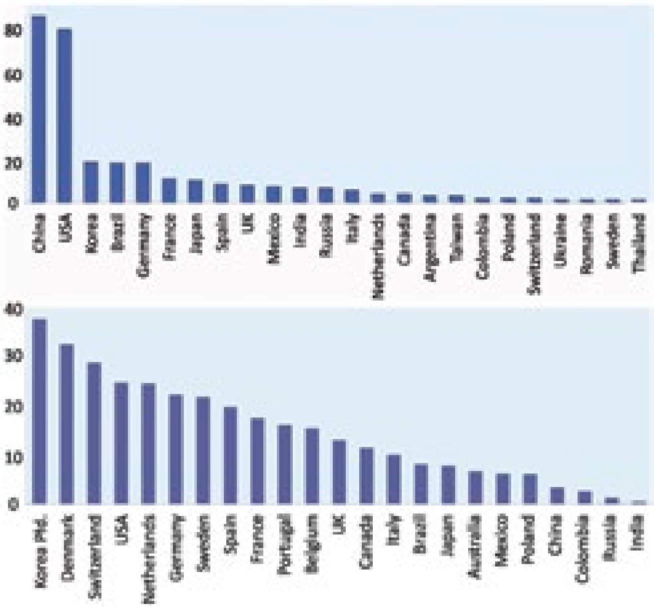

Fig. 5. The absolute number of IoT devices online (above) and the number of those devices per 100 inhabitants in 2015 [2]
Rys. 5. Bezwzględna liczba elementów w sieci IoT (wyżej) i liczba tych elementów na 100 mieszkańców w 2015 roku [2]

A peek into the future – The internet of Everything

Enthusiasts have said that that IoT will change everything, including ourselves. If this claim seems excessive, it might be worthwhile to reflect on how our lives have already been changed by the Internet – to what extent it has revolutionized education, science, the ways in which we exchange information (including our dealings with the authorities), business, commerce, medical emergency services etc. It is obviously one of the most important innovations in whole history of humanity.

The Internet of Things is likely to be to the cause of a similar revolution, affecting the daily life of entire societies. As yet we are not aware of this, just as in the 1980-ties nobody could predict the huge impact of the Internet. After all the first internet network was basically a local connection between two universities.

The Internet of Things, however, is considered only the beginning of this huge internet revolution. In May of last year, during a meeting at an open conference MobileMonday (MoMo) in Dusseldorf, specialists from Cisco Systems unveiled the concept of the Internet of Everything (IoE). As the name itself implies, IoE is a network that connects everything with everything: not only objects, but also people (by means of smartphones, laptops and tablets, as well as sensors on the skin and clothes that would be transmitting all kinds of information, for instance health – or sports-related), as well as data and processes (technological, business-related, organisation-related).

In other words, the Internet of Everything is to connect all that has not been connected before. Raymond Kurzweil – American scientist, writer, futurologist, a proponent of the idea of trans-humanism, and a pioneer in the areas of OCR, speech synthesis, speech recognition and electronic keyboard instruments, who in 2009 together with NASA and Google set up a futurology department at the Singularity University in California's Silicon Valley claimed that the pace of technological progress will be 1000 times as rapid in the 21st century as it was in the 20th. Due to explosive growth of technology in the near future not only devices that we use will be connected – everything will be connected, and to a more wider extent. In the modern world more than 99 % of things remain unconnected. The interaction of all those new people, processes, data and things within the Internet of Everything will bring unprecedented results and open up amazing possibilities.

According to Cisco the key role in the Internet of Things will be played by the Supernetwork – infrastructure that is intelligent, easy to manage, secure and scalable so that it can serve billions of devices. This intelligent network will listen, learn and react, and it will be capable of handling global data centre IP traffic in the range of 6 ZB (zettabytes, from zetta – 10^{21}).

The infrastructure and technologies of the IoT

The Internet of objects will probably become a part of our general infrastructure, which now includes running water, electricity, telephone, television and – most recent addition – the Internet. At present the technologies involved in the Internet of Things vary greatly. We are yet to reach the stage when the configuration of the network will be easy, not requiring considerable technical knowledge and expertise. In other words, it is necessary to achieve plug-and-play functionality in the IoT. The applications must run anywhere, and the infrastructure must allow the monitoring of any changes and adaptations required.

The Internet of Things is connected to the physical world. Therefore physical position and locality are very important, both for the purpose of finding particular objects and for the acquisition of knowledge. The IoT infrastructure must support the localization of objects, while at the same time ensuring security and privacy, according to the basic tenets of Information Security, including proper identification, confidentiality, data integrity, non-repudiation, authentication and authorization.

At present there is a whole host of communication technologies, both wired and wireless, and many globally accepted communication standards. These technologies will develop alongside the infrastructure and networks, and one of the driving forces of this development will be the Internet of Things. Once the entire Internet has migrated to the IPv6 standard there will be practically unlimited number of available IP addresses, allowing two-way and symmetric (true M2M) access to billions of smart things.

Here are some examples of technologies enabling the Internet of Things:

RFID and Near Field communication standards

Until 2000 RFID was the dominant standard. Later on, however, it has been overtaken by the NFC (Near Field Communication), which become common in smartphones in the early 2010-ties.

Optical labels and Quick Response (QR) codes

This technology is used for inexpensive tagging. Although smartphones can read optical codes, such as QR, the fact that a special application is required for this purpose constitutes something of an impediment.

Bluetooth Low Energy

One of the newest technologies. All the new smartphones have software that allows them to receive BLE signals. BLE tags have very low power consumption, so they can operate on the same micro battery for a year or more.

Z-Wave

Z-Wave is a low-power technology utilizing radio waves that was primarily designed for home automation for products such as lamp controllers and sensors. Optimized for reliable and low-latency communication of small data packets with data rates up to 100kbit/s, it operates in the sub-1GHz band and is impervious to interference from WiFi and other wireless technologies in the 2.4-GHz range such as Bluetooth.

Low-power wireless IP-based networks

One-chip radio transmitters using the ISM band , power-conserving WIFI version, a new, compressed version of IPv6 called 6LowPAN (IPv6 Low-power wireless Personal Area Network), and Thread, IPv6 networking protocol based on 6LowPAN and aimed at the home automation environment are the new developments in this area.

Problems and barriers

There are many problems that may impede the growth of the IoT, and they involve many different areas. Some examples are given below.

IPv6. The depletion of IPv4 addresses is already being felt – and those billions of new sensors will also require their own unique IP addresses. Therefore, widespread use of IPv6 – which, in addition to huge address space allows automatic network configuration and offers improved security functions – is a necessity. This migration to the new protocol, however, poses a number of challenges, involving such issues as compatibility (including lack of backward-compatibility with IPv4), security and privacy.

Powering the sensors. To unleash the network's full potential, the sensors must be self-reliant. It is difficult to imagine changing the batteries in billions of devices located all over the world (and even in space). Therefore, It is necessary that the sensors be capable to generate energy from their own environment – for instance, utilizing movement, light or wind (reportedly a nanogenerator converting the body's movements into electricity has already been invented)

Standards. Although many advances have already been made, there is still need for progress with regard to the issues of security, privacy, architecture and communication.

Security issues. Any application can potentially be hacked; the results can be dire enough even when the losses incurred involve data alone. In the case of the Internet of Things, however, such attacks would influence physical objects, and could. therefore, have tangible and potentially very dangerous consequences in the material world. Considering that around 70% of the 230,845 frauds recorded the US in 2013 and 2014 included a cyber element, some IT experts have already been arguing that adding more web-enabled devices to our homes might not be such a good idea. If a high level of security is not ensured – much higher, that is, than what we have at present - consumers could easily turn away from the IoT.

Costs. The cost of end devices is a key economic factor that should not be overlooked. In order to communicate by means of the IPv6 protocol an appropriate interface is required. In the case of more technically advanced devices like laptops or mobile phones its installation presents no difficulty; however, in the future the Internet of Things is to be made up largely of small, simple objects, often designed for embedding – such as sensors – the majority of which are not equipped with a processor and memory resources, and therefore not capable of storing and processing data. Such capabilities have to be provided in order to fully realize the potential of the IoT – and considering that the numbers of those devices are likely to run into billions, it is obvious that the solutions have to be very cheap.

Legal barriers. Maintaining privacy and confidentiality while using the Internet of Things is of key importance both for private individuals and companies or other organizations. The existing legal rules and regulations must be adapted to the new reality before the Internet of Things becomes a part of our everyday life. However, due to the rapidity of these changes, the state in its regulatory activities might not be able to keep up with them. For this reason in many European countries the law-making process has been decentralized, and the preparation of regulations governing network activities has been left to social and economic organizations. Apart from hastening the law-making process, this has one more positive effect - the rights and duties of network users are determined by consensus among the group interested in a given issue, which makes the law more efficient in practice. Another problem is the scope of the new regulations. It seems that national law might not be enough. As the technologies themselves know no frontiers, laws and regulations of global relevancy are required.

Perspectives and future significance of the IoT

The possibility of equipping an IoT device with a processor, memory and other resources means that internet can become of use in almost any area. The systems of the Internet of Things are not limited to passive collection of data; they can also perform many different actions. Smart commerce systems can, for instance, monitor the buying preferences of particular users by tracking the signal of their mobile phones. The same people might also receive special offers for their favourite groceries when they need them, delivered directly by their own fridge.

Other applications may provide a wide range of functions in the area of home security and automation. Even today the IoT makes it possible to control electrical devices installed in the home. Before we wake up in the morning the automated system might, for instance, make the coffee and toast the bread. And this is merely a taste of the potential capabilities of the so-called smart house – while the Internet of Things as a whole can offer much more and in many various areas. Traditional media such as newspapers, periodicals, radio or television could be replaced or enhanced with technologies that reach interested parties at the optimal time and place.

The Internet of Things allows us to collect, measure and analyse large amounts of behavioural data, that is, relating to the behaviour of people and their reactions to the stimuli in their surroundings. The use of such data might revolutionize directional marketing of products and services. Widespread adoption of the Internet of Things and Big Data technologies might usher in a new era of economic growth in the media, business, and even government administration.

Monitoring by means of the IoT network and its intelligent sensors might add a new dimension to the protection of the environment – not limited to the monitoring of air, water or soil quality, but including even such specialized observations as those of animal migrations in the wild and wildlife relocation. The authorities might use the IoT network for to provide early warning of various cataclysms, and also to deliver help for the victims in a more efficient fashion. The IoT can be used to monitor all events or changes in the infrastructure which might negatively impact security. It could also be used for repair and maintenance tasks by coordinating the activities of users and the appropriate services or authorities.

Control and management of manufacturing equipment, control of the processes of production with dynamic real-time responses - these are some other obvious applications of the Internet of Things. Intelligent production management systems might also be integrated with the Smart Grid technology, providing energy optimization in real time.

It is conceivable that electricity-powered devices within the IoT network (such as switches, sockets, bulbs, TV sets etc.) will be provided with network intelligence in order to regulate power usage. These devices will also make it possible for their users to control or manage them remotely from the cloud, as well as providing more advanced functions, such as the scheduling of power usage, turning the heating or lighting on and off remotely etc. Some such devices are already available on the market. IoT may be used in remote health monitoring systems and for the purpose of emergency alerts. This may take many different forms, from the simple monitoring of blood pressure and heart beat to the control of much more complicated devices, such as pacemakers or advanced hearing aids. Specialized sensors placed within living spaces might be used to monitor the state of health and wellbeing of the elderly, the chronically ill and small children.

In search of standards

Although at present the Internet of Things is not so much an existing product as a phenomenon in its infancy, its potential – and the challenges and problems that it is certain to cause – have already been recognized and are generating much debate. In Europe the **European Research Cluster on the Internet of Things** was established with the goal to define a common vision of the ways to realise IoT in Europe, to identify technological and developmental challenges at the European level, as well as coordinate various activities and projects, both on our continent and globally, facilitating networking and fostering communication.

Focusing in particular on the question of standards, the organization prepared – in collaboration with European and international stakeholders – the **Position Paper on Standardization for IoT** Technologies [3]**,** a technically-oriented reference document that presents the standardization requirements for the Internet of Things, the current state of the area and the existing standards, as well as an an analysis of the latter's shortcomings and recommendations for future standardisation activities. In particular, the objectives of the document were:

– to identify and present the most important activities which are to determine the points that the IoT technology has in common with other areas (cloud computing, networks, wireless protocols, identification, naming, addressing etc.)

– to map out the most important standardization initiatives for the IoT

– to analyse the similarities and differences between these initiatives;

– to determine where significant gaps exist with regard to IoT standardization solutions.

– to present recommendations with regard to future standardization efforts.

The overall goal of the document is to create the foundation for the formulation of suggestion for the future normalization activities of the IoT. The descriptive part of the document is presented in the Appendix.

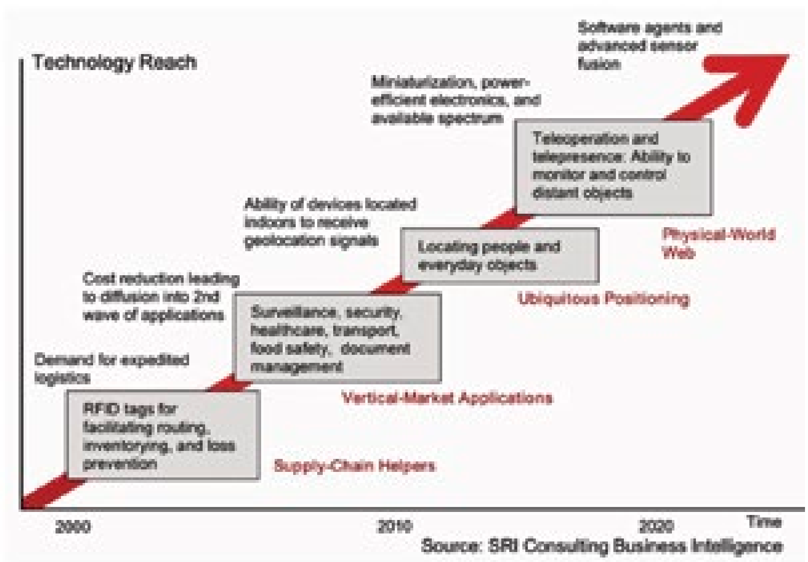

Fig. 6. Technology roadmap: the Internet oF Things
Rys. 6. „Mapa drogowa rozwoju Internetu Rzeczy wg firmy konsultingowej SRI

Literatura

[1] OECD

[2] OECD Digital Economy Outlook 2015, DOI 10.1787/888933225312

[3] Internet of Things. Position Paper on Standardization for IoT Technologies, European Research Cluster on the Internet of Things. European Communities, 2015.