Managing Innovation and Diversity
in Knowledge Society
Through Turbulent Time
25–27 May 2016
Timisoara • Romania

make learn
TIIM

Management,
Knowledge and Learning
Joint International Conference 2016
Technology, Innovation
and Industrial Management

THE INTERNET OF THINGS – SYNERGY BETWEEN VIRTUAL AND REAL WORD

Łukasz Wiechetek
Maria Curie-Sklodowska University in Lublin, Poland
lukasz.wiechetek@umcs.pl

Abstract:

The Internet of Things is a fast developing phenomenon playing an important role in more and more areas of human activity. It creates new powerful opportunities to improve efficiency, quality, accuracy and gains from the use of information systems. IoT can be also seen as an idea of strengthening the link between virtual and real world that creates and amplifies many synergy effects. Due to its power, size, value, possibilities but also threats of use, IoT should be (now and in the near future) one of main concerns of both regulators, managers, administration representatives and casual users. The publication presents the results of literature research in the area of synergy effects created by Internet of Things. The author discusses IoT not only from the technical point of view but tries to build a holistic ecosystem consisting of technical, economical, educational, law and social components. The main parts of the article are: IoT as interconnection between virtual and real world, IoT application areas, advantages and threats of IoT, regulation issues and finally some predictions about the future IoT development. The research shows that IoT is an important phenomenon, and will be even more important in near future, especially in the areas of process automation, infrastructure management, marketing, object tracking, education, and ICT law. IoT is also a great opportunity for developing countries (e.g. its appearance in global trade), gives also the ability to reduce the importance of cultural differences in international cooperation. It allows running and or strengthening many synergy effects. However power of strong interconnection between virtual and real world can be not only a source of new possibilities but also brings concerns and problems especially in the area of privacy, security and intellectual property. IoT future development is inevitable and should be seen as a next step of the information revolution.

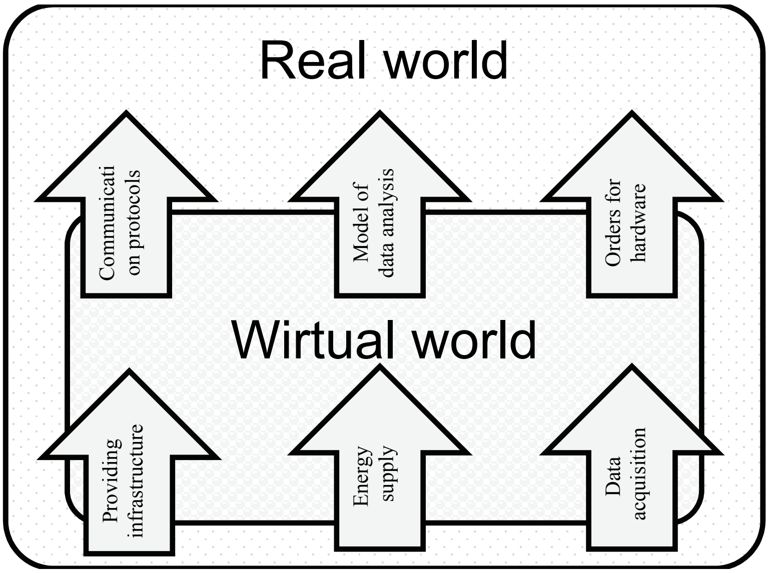
Keywords: IoT, Internet of Things, synergy, Internet of Everything, IoE, Machine to Machine, M2M

1. INTRODUCTION TO THE INTERNET OF THINGS

The Internet is a central point of human activity: amusement (internet games, social networks, online video, television on demand, health & fitness (Puppet 2014, p. 86)), education (e-learning platforms, virtual words, and virtual laboratories) (Cornel 2015, p. 57), work (teleworking, telecentres, home offices) (Macaulay et al. 2015, p. 3). However over the past few years The Internet tends to a play role of global communication network not only for people but also for things: cars, planes, smartphones, washing machines, refrigerators, TV sets, buildings, and many others. Recently it has gained much attention from researchers, practitioners and policy makers (Xia et al. 2012, p. 1101). It became important theme in books, conferences, seminars, journals, research programmes, school courses (Fleisch 2010, p. 126).

The Internet of Things (IoT) can be defined as a concept that some precisely identified objects equipped with sensors (ubiquitous intelligence) can collect and exchange data using computer network (Xia et al. 2012, p. 1101), (Skinner 2013, p. 204), (Graham and Haarstad 2011, p. 6). The IoT functional objects can be automatically identified and tracked (Xu, 2011, p. 188). That kind of network create opportunities to improve efficiency (Macaulay et al. 2015, p. 8), quality, accuracy and gains from the use of information systems (Kopetz 2011, p. 309). IoT can be therefore seen as a link between virtual and real word (**picture 1**).

Picture 1: IoT as interconnection between virtual and real world



Source: own work.

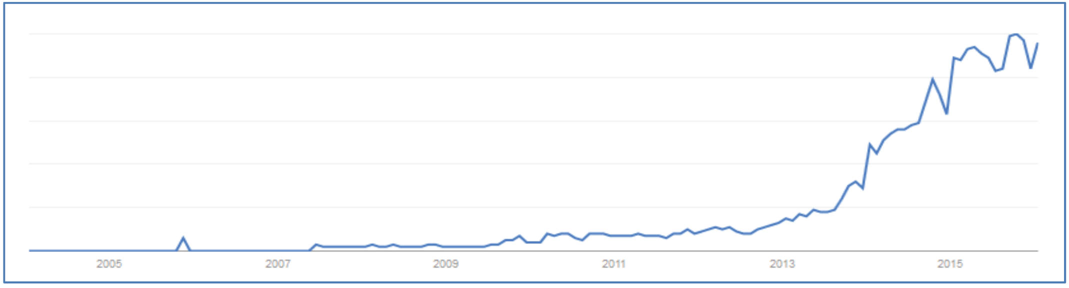
On the one hand hardware units (sensors, detectors, receptors, and appliances) automatically feed virtual components of the system with large amount of real-time collected data (Mishler 2015, p. 62). On the other hand data transmitted and transformed in virtual world (clouds, big data) become the instructions, guidelines, orders for hardware units. Due to that cooperation some synergy effects are created. These effects provide great opportunities for the Internet of Things. However, they may also lead to many threats in the area of: discrimination, privacy, security and consent, surveillance, bias (Dobrian 2015, p. 11), (Waltzman and Lei 2015, p. 19), (Puppet 2014, pp. 117-147), (Khoo 2014, p. 2), (Bradley et al. 2014, p.16), (Graham and Haarstad 2011, p. 13).

The idea of communicating hardware objects is not new, and occurred even before the Internet, about 50 years ago (OECD 2015, p. 240). The term IoT was coined by Kevin Ashton in 1999 (The Guardian, 2015) and was used to characterize the manner in which network connected devices can change the way of life. Ashton claimed that the foundation for IoT developement was radio-frequency identification (RFID) technology. With the help of RFID many processes could be automated (Wikipedia 2015). Previous term used by OECD to define »*devices that are actively communicationg using wired and wireless network, that are not computers in the traditional sense and are using the Internet in some form or another*« (OECD, 2015, p. 242) was machine-to-machine communication (M2M). According to OECD reports IoT includes all new trends in M2M: clouds, big data, sensors and people, and plays important role in most sectors of the economy: industrial procesesses, customer services, home services, transportation systems, health care, public services (OECD, 2015, p. 240).

IoT has great potential and power. It can connect and automate almost everything from everyday use gadgets (wearable devices), via home appliances to entire buildings, factories and cities.

The extension of the IoT term is *Internet of Everything (IoE) formulated by CISCO company. IoE means the set of people, processes, data and things connectet to the Internet* (Macaulay et al. 2015, p. 5), (O'leary 2013, pp. 53-54). The term IoT became popular in 2010. For the past three years interest in IoT increased rapidly mainly due to: technology development, lowering cost of development and deployment (Saint 2015, p. 74), increase of user awareness and great synergy opportunities offered by combining virtual and real world. According to GoogleTrends **(picture 2)**, the increase between 2013 and 2014 was almost three times, and between 2014 and 2015 almost doubled.

Picture 2: Interest in the topic Internet of Things in terms of time (%)



Source: Google Trends, https://www.google.pl/trends/explore#q=%22internet+of+things%22 (12.01.2016).

Nowadays not only IT specialists but also managers, policy makers, regulators claims that the Internet of Things can be a great leap in convergence between ICT and the economy (OECD 2015, p. 240).

We can give a lot of examples of new business ideas related to IoT. The IoT projects are quite innovative, sometimes very risky so may face problems of financing. Sometimes only way to finance them is crowdfunding. One of the leading crowdfunding platform is Kickstarter (www.kickstarter.com). The number of creative IoT projects on Kickstarter platform can be used as an indicator of interest in IoT and show trends of its development. At present we can find there 65 IoT related projects. Characteristics of sample IoT related project presented on Kickstarter were showed in **table 1**.

Table 1: Characteristics of sample Kickstarter IoT related project

No	Name	Description
1	Complete Arduino IoT WiFi Controller	Complete IoT Programmable Logic Controller, ready to run. It can be used for: home automation and security, robotics & machine control, industrial automation, 3-D printing or educational purposes.
2	riots	A plug-n-play Arduino compatible wireless network of sensors and controllers with an integrated cloud interface.
3	ioXtreme	Robust modular mounting system for IoT Controllers e.g. Raspberry PI, Arduino, Beaglebone.
4	The IoT Relay	Durable, safe and reliable power control for creating the Internet of Things.
5	Creator Ci40	IoT kit (hardware, software, and cloud infrastructure) needed to build a wireless IoT system.
6	LimiFrog	Programmable module for inventing and prototyping smart objects with sensors, strong MCU, bluetooth, oled.
7	Esquilo	A development platform with built-in Wi-Fi, web IDE, cloud access, Arduino shield.
8	CybatiWorks	Academic and professional control system and interactive educational platform for home use, industry and educational institutions. Presenting materials about how critical infrastructure works and how to defend it.
9	Vigek IOT Core	Smart IoT platform that can take photos. Cheap, small, modular, and APP controlled IoT development board that brings Wi-Fi and camera together.
10	IoT Village	Set of workshops on hacking numerous off-the-shelf devices including medical devices, home appliances, routers, storage devices. Delivers security advancements in Internet of Things devices.

Source: www.kickstarter.com (13.01.2016).

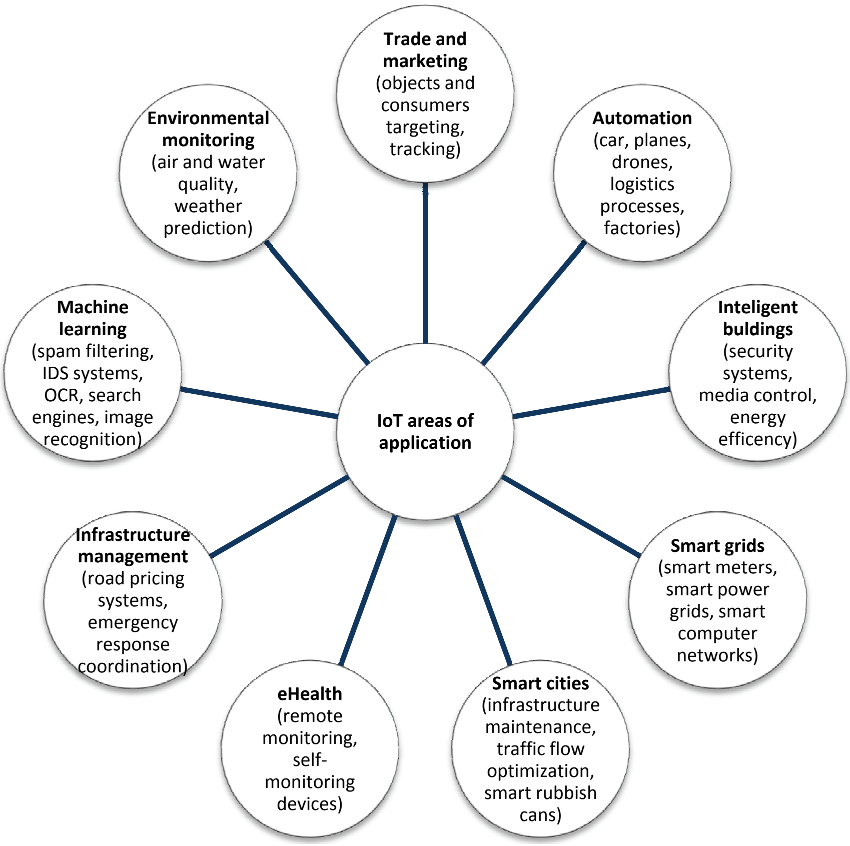
After analysing over sixty IoT related projects described on Kickstarter there can be concluded that at present the areas of Internet of Thing development are much diversified. From complex hardware kits for building IoT systems, IoT networks for whole cities, big industry; through educational platforms on IoT, tracking and monitoring tools; to small, easy to use everyday gadgets. However they seem to have some similar features. They are small, energy-efficient, easy to use, and easy to reconfigure. They use similar technologies e.g.: Wi-Fi, Bluetooth, NFC, Arduino components. Many of present IoT solutions are open-source (Munk 2015, p. 12). The synergy effects created by IoT are often supported with wide wireless communication standards as Wi-Fi, Bluetooth but also availability and openness of source code that allows for easy customization and configuration.

The IoT market grows up rapidly. OECD estimates that today's family of four (two adults plus two teenagers) uses 10 internet connected devices (OECD 2015, p. 255). One of the estimator of IoT size can be number of used SIM cards. According to data presented by International Telecommunication Union, in May 2014 there were 6.9 billion mobile cellular subscriptions (ITU 2015). In 2013 there were 14 countries with over 100 million mobile subscriptions. The highest number of subscriptions was reported in: China, India, USA, Indonesia, Brazil, Russia, and Japan (MobiForge 2014).

2. THE MAIN AREAS OF USING IOT

The IoT sollutions can be used in many areas of people's activity: entertainment, education and work (Kopetz 2011, p. 307). Using IoT we can increase the ubiquity of the Internet (Xia et al. 2012, p.1101). At the micro level IoT can be very useful for households, increasing, improving the convenience, comfort and security of life (Kolenda 2015, pp. 11-15). In the intermediate scale it can act as a regulator of manufacturing processes, support medical heath care or be used by companies for consumer and objects targeting or tracking (Graham and Haarstad 2011, p. 6). Finally in the macro scale IoT is used to build smart cities, automated wide area logistics networks, building unmanned transportation systems or infrastructure or smart energy management systems (Lodder & Wisman, 2015, p. 20). Main areas of IoT usage were presented on **picture 3**.

Picture 3: IoT areas of use


IoT areas of application
Trade and marketing (objects and consumers targeting, tracking)
Automation (car, planes, drones, logistics processes, factories)
Inteligent buldings (security systems, media control, energy efficency)
Smart grids (smart meters, smart power grids, smart computer networks)
Smart cities (infrastructure maintenance, traffic flow optimization, smart rubbish cans)
eHealth (remote monitoring, self-monitoring devices)
Infrastructure management (road pricing systems, emergency response coordination)
Machine learning (spam filtering, IDS systems, OCR, search engines, image recognition)
Environmental monitoring (air and water quality, weather prediction)

Source: own work.

As we can see the range of IoT application is very wide. Modern technology development, the growing needs of people, businesses, cities, local governments and countries create the conditions for a rapid development of Internet of Things. Apparently, in the near future we will observe growth of IoT market not only in terms of quantity (increase in the number of devices) but also in qualitative terms (new fields of application) (Kopetz 2011, p. 309), (Macaulay et al. 2015, p. 13).

3. ADVANTAGES AND THREATS OF IOT

The full set of the advantages and threats of IoT is hard to present because every day there are created new IoT solutions, meet emerging needs and opening new concerns. However it is worth to say that development of IoT is a great chance for developing countries where great changes in infrastructure (e.g. roads, power grids, public buildings, government buildings, culture centres) but also post-industrial into information society transformation are natural path of growth. Using IoT solutions and putting efforts on education in the area of IT, economies can develop not only in an evolutionary way but make a real leap forward.

According to OECD reports (OECD 2015, p. 247) the key advantages of using IoT in the area of transport automation are: utilisation (using for majority of lifetime), energy efficiency, increase in safety and empowerment (require less skills to use). Analyses of the sectoral reports and scientific publications allows to say, that the main advantages of using IoT are:

- collecting near real-time, detailed information, obtained automatically,
- possibility of a quick response to incoming signals,
- stronger integration between the real world and world of the of information systems (better data quality) (Kopetz 2011, p. 312),
- ability for real-time quality management and control (Xu, 2011, p. 183),
- opportunity for better monitoring, controlling, automation intelligent things (Kolenda 2015, pp. 11-15),
- central management of appliances via remote control or cloud,
- billing only for effective usage (energy, telecommunication, transportation),
- faster and automated changing of the supplier,
- machinery awareness of its own condition (Mishler 2015, p. 63),
- opportunity to leverage the power of the physical world (Fleisch 2010, p. 148),
- people and object traceability (Pye 2014, p. 65),
- wider information access, more transparent organizations,
- facilitation the exchange of goods and services (Weber & Weber 2010, p.III),
- expansion of developing countries in global trade (Weber & Weber 2010, p.III),
- facilitation the fight against counterfeiting,
- possibility for competition stimulation with the inclusion of more trade participants,
- opportunity to reduce the importance of cultural differences in international trade by processes automation,
- better labour conditions and labour standards monitoring,
- the chance to improve the quality of live (Xia et al. 2012, p. 1101),
- possibility for quick change in life-style (Kopetz 2011, p. 311), (Hu 2011, p. 2451).

Huge networks consisted of great number of appliances, generating enormous amounts of data can unfortunately lead to many problems and threats. The source of many hazards related to IoT can also be the excessive trust in “intelligent” hardware and the fading of basic (natural) skills due to the high level of automation. Cyber-attacks on IoT can be very harmful, causing not only virtual but also physical damages in real world (Clearfield 2013, p. 1). Analysed publications presents many examples of treats caused by IoT, e.g.:

- serious privacy treats (Kolenda 2015, pp. 27),and possibility of political manipulation,
- possibility of spying on people even in their own homes,
- unauthorized remote access to IoT devices (leak of company, personal or health information) (Dobrian 2015, p. 11),
- using wearable devices as a spy tools,
- lock of processes, companies and even entire cities through the acquisition of control of the infrastructure for IoT,
- remote controlled units (unmanned cars or drones) used for a terrorist attacks,
- take control over man, by machine (Kolenda 2015, pp. 27),
- caring out a high-volume DDoS attack using IoT devices.

According to CISCO reports from 2000 to 2015 IT security specialists informed about many attacks on power plants monitoring systems, automobile manufacturing plants, trains and trams monitoring systems, water treatment facilities, increased cyber espionage campaign (CISCO 2015, p. 2).

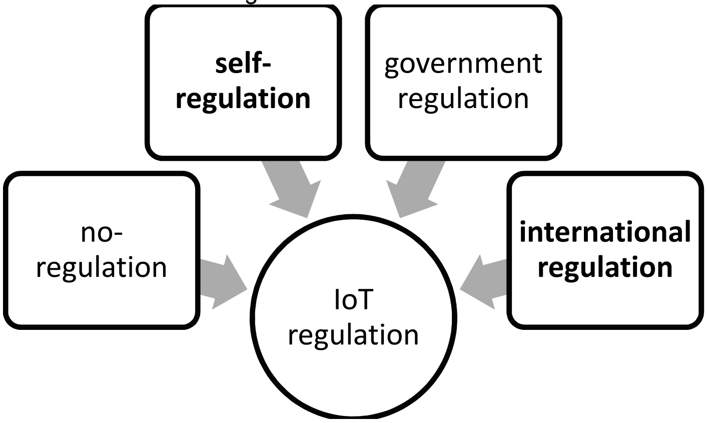
IoT like every new technology can be the source of many opportunities but also generates new treats. The mentioned dangers are particularly serious because of the vast number of attacked users, but also due to damages caused not only in the virtual but also in real world.

4. THE INTERNET OF THINGS REGULATION AND POLICY

Development of IoT is possible with the support of accurate technology, actors wanting to use it (equipped with appropriate knowledge and skills), the economic rationales (operational efficiency, competitive advantage) (Macaulay et al. 2015, p. 7), (Mishler 2015, p. 62), the company culture to be truly innovative (Weinman 2015, p. 16), but also appropriate regulation, policy providing standards, facilitating the use of IoT, increasing the security (safety) level and ensuring privacy. Regulatory framework should provide at least security of the structure and privacy of users (Weber & Weber p. 3), and lead to a win-win situation for both business and consumers (Zhou 2015, p. 29). Policy makers realized that interconnection of virtual and real world has immense power and offers numerous opportunities. However this new force can be used for the sake of humanity but also may become a destructive weapon controlled by the unauthorized persons or organizations. Therefore it is necessary to create and implement policy, also IoT risk-based security programs and distribute it among stakeholders (CISCO 2015, p. 5).

Creation of suitable law frameworks in the area of IoT is a big challenge because it requires setting up the rules for functioning virtual and real world. The possible models of legal framework in the area of IoT could be as follows: no-regulation, government regulation, self-regulation and finally international regulation (**picture 4**).

Picture 4: Models of IoT regulation



Source: Weber & Weber, 2010, p. 23.

No-regulation model should be discarded mainly due to the importance, size and value of IoT phenomenon, derived from synergy effects created thorough cooperation between virtual and real world. Secondly, Internet of Things can be used to support global (logistics, environmental, social, marketing (Mancuso 2015, p. 16)) processes that is why preparing regulations by separate governments may cause a lot of problems like coherence of many acts, and territorial restrictions, so this model should also be rejected.

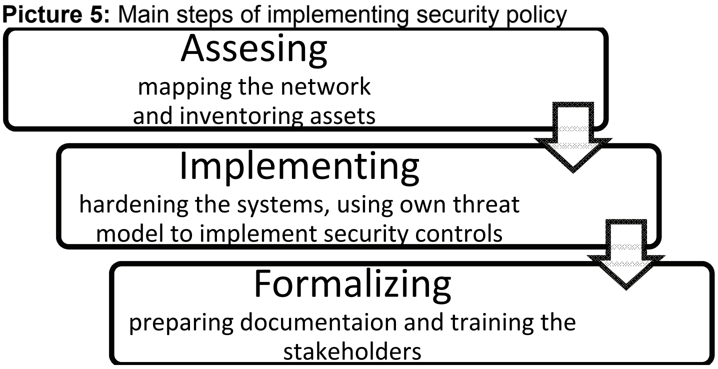
More suitable models are self-regulation and international regulation. Self-regulation can be seen as social control so very powerful and efficient mechanism. It is not imposed by the authority, needs the involvement of concerned people but reflects the real needs. That is why legal framework should be built mainly in self-regulation model.

International regulation model needs an international regulator that sometimes it is hard to choose. The regulatory body can also be newly created as a set of government, business, scholar, NGO representatives. However, creation of new international body takes a lot of time and can be great obstacle from fast developing IoT market point of view. Some regulatory bodies could also be created inside of existing international organizations like WTO, OECD. Finally we can imagine regional regulators like European Union Commission. OECD claims that international organizations, countries should promote IoT-driven economic development (OECD 2015, p. 262).

Legal framework should be prepared and implemented before IoT is fully operable (Weber & Weber p. 3). The history of ICT technologies development unfortunately shows that legislation does not always keep pace with the introduction of new IT solutions (Puppet 2014, pp. 136-139). For example, according to OECD report at present countries don't have regulations that allows to use autonomous or remote controlled machines (planes, cars) (OECD 2015, p. 272). However some countries allows for using Unmanned Aerial Vehicles or drones. That delay creates the gap, the source of many users' concerns and the opportunity for unfair entrepreneurs and criminal organizations to misuse the Internet of Things synergy forces and creates a bad climate for IoT development.

Global regulatory framework should oblige suppliers and users IoT to develop security polices improving the safety of IT infrastructure. According to CISCO the security policy should consist of three steps: assets inventorying, systems hardening and formalization of procedures **(picture 5)**.

Picture 5: Main steps of implementing security policy


Assesing
mapping the network and inventoring assets
Implementing
hardening the systems, using own threat model to implement security controls
Formalizing
preparing documentaion and training the stakeholders

Source: Cisco, 2015, p. 6.

Inventorying assets is obligatory due to the large number and dispersion of IoT equipment. IoT network can be built in unique way and perform and offer highly specialized functionalities. Therefore the system should be harden using own threat model. Finally, collected information and prepared procedures should be transformed into documentation for easy distribution and reuse.

Policy concerns should focus not only on security issues but involve a much wider range. Economists claim that rapid development of machine to machine communication and automation can lead to friction problems in the economy. Some standardized, routine jobs in finance, law, and consultancy may disappear. That is why policy makers should think it over in detail.

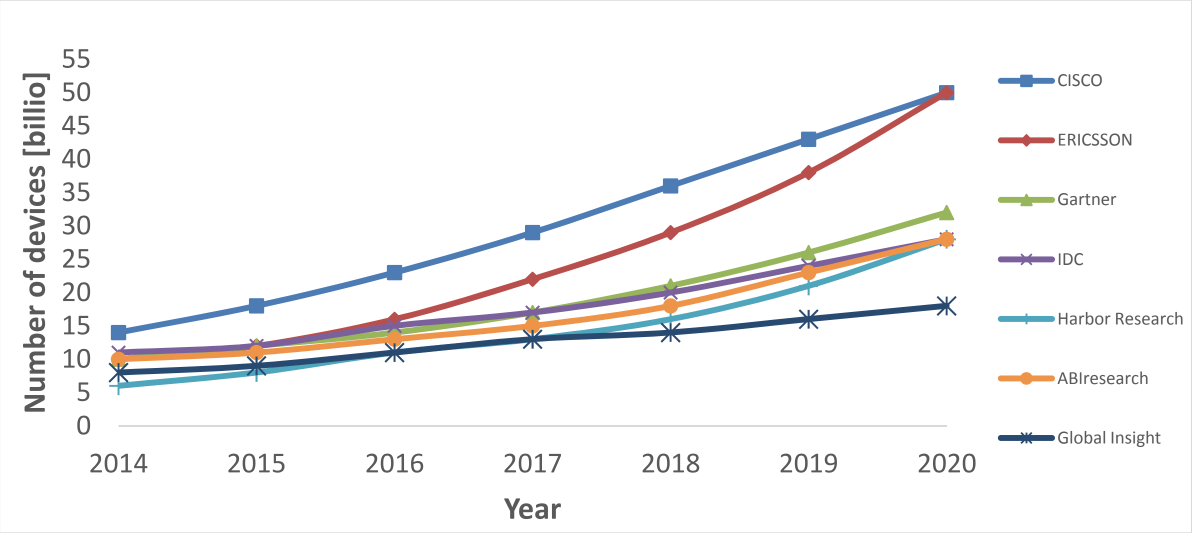
Finally the most appropriate models of IoT regulatory should be built on social control (self-regulation) and combined with internationally created legal framework (international regulation), ensuring law coherence. Good law should provide the security and protection of privacy. However it is worth to remember that safety chain is only as strong as its weakest link. So in order to protect opportunities derived from synergy of virtual and real world all stakeholders should build appropriate policy in accordance with the established law and internal regulations.

5. THE FUTURE OF IOT

Internet of Things will develop rapidly in the next years. It can provide both automation, transformation and information effects (Boos et al. 2013, pp. 445-446). Experts say that IoT is a next step of the industrial (Ng 2015, p. 6), security and information revolution. Mostly due to technical issues: improving communication technologies, energy consumption reduction, creation of commonly accepted standards; economic reasons: cost reduction, increase in life time of hardware but also due to social reasons like: improving quality of life, development of information society. Finally, the society members should be equipped with appropriate knowledge, skills but also should trust and want to use IoT solutions.

The present and future size of IoT is hard to calculate. Nowadays the volume of traffic in the internet doubles every 18 months (Skinner 2013, p. 203). The Gartner forecasts shows that by 2020 there will be 26 billion units (Gartner 2013) and will become a multi-trillion dollar market (Lueth 2014). The Worldwide Internet of Things revenue by 2020 will be 7 trillion dollars (Lund et al. 2014, p. 23). Big players on IoT market like Ericson, Cisco estimated that by 2020 there will be about 50 billion devices connected to the Internet (Macaulay et al. 2015, p. 4) (**picture 6**). When we assume that the population of the world in 2020 will be 7.7 billion it gives about 6.5 devices per person. According to The Forrester Research IoT revenues will be 30 times of the Internet (Pye 2014, p. 65).

Picture 6: Worldwide IoT connected devices (forecast)



Source: Lueth, K. L., 2014.

The main reasons for IoT development can be:

- desire of people to make life simpler,
- creation of new applications,
- benefits derived from the possibility of analysing and linking great amount of data in real time using big data and cloud computing,
- possibility of preparing personalized offer for individual customer,
- preparation user awareness-raising campaigns in the area of IoT (Brown 2015, p. 32),
- increase in high quality of services and fair business practices of IoT suppliers and supervisors,
- decrease in costs of IoT infrastructure and deployment,
- popularity of smartphones equipped with wide communication capabilities: Wi-Fi, Bluetooth, NFC that can be used as IoT sensors,
- production of appliances like, TV sets, radio, speakers, bulbs that can be controlled via Internet,
- increasing level of interoperability of connected appliance,
- development new low-energy consuming technologies like Bluetooth 4.0, low rate wireless personal area network,
- development and standardisation of communication technology for short range like NFC, Bluetooth, IEEE 802.15.4 (low rate wireless personal area network), Wi-Fi, but also for wide range 2G/3G/4G networks, IPv6,
- development and implementing privacy management standards, programmes and privacy enhancing technologies,
- cooperation of users, companies and governments in the area of cybersecurity,
- enhancing user knowledge, skills and experience, building the vision of Internet of Things as Internet of Trust,
- enhancing by the governments knowledge and skills in the area of IoT security.

As we can see future growth of IoT will be determined not only by technical issues but also economy rationale and the natural tendency of people to facilitate their lives. The increase rate can be supported through appropriate policies that can force or encourage people to use IoT through building vision of safe and easy to use IoT world.

Nowadays IoT stakeholders are facing persistent threats that due to the openness and disperse of systems are more sophisticated, widespread. These treats because of synergy effects created by IoT can cause significant economic, social, environmental damage both in virtual and real world e.g. process interruption, power grid disruption and physical injury (Cisco 2015, p. 1). Therefore the future development of IoT can be decelerated mostly due to:

- lack of awareness of existing IoT solutions,
- security concerns as one of the most important issues (Xia et al. 2012, p. 1102),

- ethics concern, ensuring: property rights, access to information, integrity of information (Popescul and Georgescu 2013, p. 211),
- the fear of disclosure of private data,
- fear of onward use of collected data outside the initial terms of contract,
- wider possibility of intellectual property theft (Bradley et al. 2014, p.16),
- fear of replacing people by intelligent machines (automata) that could increase unemployment and conduct to recession,
- public safety concerns,
- brand damage of companies using compromised IoT solutions,
- lost of trust to service providers,
- complicated deployment of IoT components,
- problems with providing efficient power supply to millions of connected devices (Ng 2014, p. 14),
- difficulties related to standardisation (instead of one worldwide standard few manufacturers competing standards),
- conflicts with existing regulations.

The main obstacles to IoT development therefore, lie in security and privacy issues (Saint 2015, p. 74) but also in the absence of appropriate regulations and standards that precisely define the rights and obligations of IoT market stakeholders. The overcoming these barriers require changes in education, especially in the area of creating and exploiting new IoT related technologies (Xia et al. 2012, p. 1101), (Popescul and Georgescu 2013, p. 213).

CONCLUSION

We can conclude that Internet of things has grown significantly over the past few years and will be growing in the future. IoT creates great opportunities for improving: quality, reliability, accuracy of IT systems especially due to strong link, feedback created between virtual and real word. This link starts synergy effects derived from the automation in data collection, processing and communication. Nowadays IoT solutions are used especially in the area of: intelligent buildings, smart grids and smart cities, environment monitoring (Postolache et al. 2014, p. 610), (Hu 2011, p. 2451-2454), infrastructure management. The future of IoT seems to be great qualitative and quantitative growth. IoT opens many new opportunities for: real-time systems, effective energy usage, transparency of systems and organizations, global trade and fight against counterfeiting. However can also bring concerns and problems:

- privacy issues, by passing automatically very detailed information about the user;
- concerns about restricted information that should not be communicated. Unfortunately at present we are not quite sure what information can be used in what way, so can’t precisely decide what data should be private, public, or maybe accessible in protected mode;
- needs for establishing legal framework in the way that allows flexibility but also has a power to create internationally respected and coherent rules.

For present IoT users (consumers) the main concern is privacy and security. If the IoT processes work automatically the questions are: What and when data are being collected? What are the purposes for data collecting? Who will be able to use the data? and Is the whole system secure?

Using, supporting the IoT systems also requires creation of rules for improving appropriate security policies. Growth of IoT market is determined not only by technical, security and economical, legal issues. To release full synergy effects accumulated in the Internet of things it is also necessary to implement an appropriate education policy convincing business and people to IoT, forming and enhancing the information society.

One thing is for sure, IoT due to its size, value, possibilities should be one of the main concerns of regulators, managers, business and administration representatives, but also common users. The Internet of Things phenomenon is also new, developing, slightly examined area of science and should become of great interest for scientists representing many disciplines (Dlodlo 2012, p. 256): computer science, economics, management, sociology, psychology. The future research in the area of IoT could be concentrated on exploring attitudes towards IT among both individual consumers, managers as well as representatives of the administration (Possibly with the use of The Technology Acceptance Model (TAM)). Second issue may concern the impact of legislation on the direction and rate of the Internet of Things development. Finally an interesting topic is a comparative study of the IoT development paths both in poor, developing and developed economies.

REFERENCE

1. Boos D. and Guenter, H. and Grote, G. and Kinder, K. (2013). Controllable accountabilities: the Internet of Things and its challenges for organisations. *Behaviour & Information Technology*, 32(5), 449-467.
2. Bradley, T. and Thibodeau, P. and Ng, V. (2014). The Internet of Things -- threats and challenges. *NetworkWorld Asia*, 11(1), 16-18.
3. Brown, E. (2015). Internet law in the courts. *Journal of Internet Law*, 18(11), 30-33.
4. Cisco (2015). IoT Threat Environment, An overview of the IoT threat landscape with risk -based security program recommendations. Retrieved from http://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/C11-735871.pdf.
5. Clearfield, Ch. (2013). Rethinking Security for the Internet of Things. Harvard Business Review. Retrieved from https://hbr.org/2013/06/rethinking-security-for-the-in.
6. Cornel, C.-E. (2015). New techniques for implementing online virtual laboratories. *Internal Auditing & Risk Management*, 10(3), 55-63.
7. Dlodlo, N. and Foko, T., and Mvelase, P. and Mathaba, S. (2012). The State of Affairs in Internet of Things Research. *Electronic Journal of Information Systems Evaluation*, 15(3), 244-258.
8. Dobrian, J. (2015). Are you sitting on a cyber security bombshell? *Journal of Property Management*, 80(5), 8-11.
9. Fleisch, E. (2010). What is the Internet of Things? An economic perspective. *Economics, Management & Financial Markets*, 5(2), 125-157.
10. Gartner (2015). Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. Retrieved from http://www.gartner.com/newsroom/id/2636073.
11. Graham, M. and Haarstad, H. (2011). Transparency and Development: Ethical Consumption Through Web 2.0 and the Internet of Things. I*nformation Technologies & International Development*, 7(1), 1-18.
12. Hu, H. and Yang, D. and Fu, L. and Xiang, H., Fu, C. and Sang, J. and Ye, C. and Li, R. (2011). Semantic Web-based policy interaction detection method with rules in smart home for detecting interactions among user policies. *IET Communications*, 5(17), 2451-2460.
13. International Telecommunication Union (ITU) (2015). ITU Yearbook of Statistics 2015. Retrieved from https://mobiforge.com/research-analysis/global-mobile-statistics-2014-part-a-mobile-subscribers-handset-market-share-mobile-operators#subscribers.
14. Khoo, B. L. (2014). Going for growth with IT. *NetworkWorld Asia*, 11(1), p. 2.
15. Kolenda, P. (ed.), (2015). Internet Rzeczy w Polsce, IAB Polska. Retrieved from http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf.
16. Kopetz, H. (2011). Design Principles for Distributed Embedded Applications. New York Dordrecht Heidelberg London: Springer.
17. Lodder, A. R., & Wisman, T. H. A. (2015). Artificial intelligence techniques and the smart grid: towards smart meter convenience while maintaining privacy. *Journal of Internet Law*, 19(6), 20-27.
18. Lueth, K. L. (2014), IoT Market – Forecasts at a glance. IoT Analytics. Retrieved from: http://iot-analytics.com/iot-market-forecasts-overview/.
19. Lund, D. and Turner, V. and MacGillivray, C. and Morales, M. (2014). Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand. IDC. Retrieved from: http://www.business.att.com/content/article/IoT-worldwide_regional_2014-2020-forecast.pdf.
20. Macaulay, J. and Buckalew, L. and Chung, G. (2015). Internet of Things in logistics, DHL Trend Research/Cisco Consulting Services. Retrieved from: http://www.dhl.com/content/dam/Local_Images/g0/New_aboutus/innovation/DHLTrendReport_Internet_of_things.pdf.
21. Mancuso, J. and Stuth, C. (2015). The Internet of All Things. *Marketing Insights*, 27(2), 16-17. Mishler, Ch. (2015). The future of the Internet of Things. *Strategic Finance,* 97(11), 62-63.
22. MobiForge (2014). Global mobile statistics 2014 Part A: Mobile subscribers; handset market share; mobile operators. Retrieved from: https://mobiforge.com/research-analysis/global-mobile-statistics-2014-part-a-mobile-subscribers-handset-market-share-mobile-operators#subscribers.
23. Munk, S. (2015). Internet of Things devices go open source. *Engineering & Technology*, 10(1), 12.
24. Ng, V. (2015). Enabling the new industrial revolution, *NetworkWorld Asia*, 12(1), 6-7.

25. Ng, V. (2014). Drivers and obstacles to IoT adoption in Asia Pacific. *NetworkWorld Asia*, 11(3), 12-14.
26. OECD (2015). OECD Digital Economy Outlook 2015. Emerging issues: The Internet of Things, Retrieved from http://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2015/emerging-issues-the-internet-of-things_9789264232440-8-en;jsessionid=2p3ao26t7xd08.x-oecd-live-02.
27. O'leary D. E. (2013). 'Big data', the 'Internet of Things' and the 'Internet of Signs'. *Intelligent Systems in Accounting*, *Finance & Management*, 20(1), 53-65.
28. Peppet, S. R. (2014). Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, 93(1), 85-178.
29. Popescul, D. and Georgescu, M. (2013). Internet of Things - some ethical issues. *USV Annals of Economics & Public Administration*, 13(2), 208-214.
30. Postolache, O. and Pereira, J. D. and Girão, P. S. (2014). Wireless sensor network-based solution for environmental monitoring: water quality assessment case study. *IET Science, Measurement & Technology*, 8(6), 610-616.
31. Pye, A. (2014). The Internet of Things connecting the unconnected. *Engineering & Technology*, 9(11), 64-70.
32. Saint, A. (2015). Where next for the Internet of Things? *Engineering & Technology*, 10(1), 72-75.
33. Skinner, Ch. (2013). The future is all about the data. *Journal of Payments Strategy & Systems*, 7(3), 203-210.
34. Waltzman, H. W. and Lei, S. (2015). The Internet of Things. *Intellectual Property & Technology Law Journal*, 27(7), 19-21.
35. Weber, R. H., Weber, R. (2010). Internet of Things Legal Perspectives. Zurich – Basel – Geneva: Springer.
36. Weinman, J. (2015). Digital Technologies and Competitive Advantage. *Research Technology Management*, 58(6), 12-17.
37. Wikipedia. The Internet of Things. Retrieved from https://en.wikipedia.org/wiki/Internet_of_Things#cite_note-10.
38. Wood, A. (2015). The internet of things is revolutionising our lives, but standards are a must, *The Guardian*. Retrieved from http://www.theguardian.com/media-network/2015/mar/31/the-internet-of-things-is-revolutionising-our-lives-but-standards-are-a-must.
39. Xia, F., Yang, L. T., Wang, L., Vinel, A. (2012). Internet of Things. *International Journal of Communication Systems*, 25, 1101-1012.
40. Xu, L. D. (2011). Information architecture for supply chain quality management. *International Journal of Production Research*, 49(1), 183-198.
41. Zhou, W. and Piramuthu, S. (2015). Information Relevance Model of Customized Privacy for IoT. *Journal of Business Ethics*, 131(1), 19-30.