THE ROLE OF INTERNET OF THINGS IN DEVELOPING SMART CITIES

Andreea-Maria Tirziu[1] and Catalin Vrabie[2]

DOI: 10.24989/ocg.v331.22

Abstract
A main characteristic of smart cities is the use of information and communications technology in all aspects of city life. In this regard, Internet of Things (IoT) is a core element in the process of developing communities "ruled" by an improved communication, better understanding and wait times decrease. This paper aims to present the ways in which IoT networks and services can contribute to develop smart cities, giving as example various cities that have implemented this concept. The methodology used to carry out this research is both bibliographic – opting here to study the work of specialists in the field, authors from Romania and abroad, and empirical – formed by a case study on various smart cities around the world that use IoT. This type of smart cities is starting to transform all public institutions, changing their culture, from one control-based to one performance-centered. IoT is starting to play an important role in smart cities' evolution and it brings an improvement in the government-citizens relationship. We have identified that although technology is a central element, there should also be considered the capability and willingness of citizens and public institutions to collaborate in order to implement the best solutions for the communities.

1. Introduction

We consider important to firstly mention the research question of this paper, which is the following one: „Is there any missing link between the Internet of Things and the development of smart cities and, if yes, what might that link be?". The information presented in this article will be of aid in finding an answer to this question.

The Internet of Things concept (known in the literature as IoT) is not as new as one might think. It first appeared in 1999 when Kevin Ashton, the British who created the RFID (Radio Frequency Identification) systems standards, used it to describe a system in which the Internet connects to the physical world through sensors [2], these having the role of collecting data for sending them over networks to servers. Since back then he described how the devices connected to the Internet will change our lives, which nowadays is already far from being science-fiction. We see everywhere around us either cars connected to the Internet (via GPS terminals installed on board), industrial or agricultural equipment remotely coordinated through the Internet, drones, even refrigerators and washing machines (the smart mobile phones, present in everyone's pocket, are the best proof of the development of this IT industry's segment).

Today, the total number of connected equipment reached 23.14 billion, with the prospect of reaching 75.44 billion in 2025 [19].

[1] SNSPA, Bucharest, Romania, e-mail: tirziu.andreea@yahoo.com
[2] SNSPA, Bucharest, Romania, e-mail: cataloi@yahoo.com

The main components of an IoT system are the following [22]:

- **Data collection equipment** – some examples here would be: sensors, mobile phones, etc.;
- **Communication networks** with the role of connecting the equipment mentioned above – such as Wi-Fi, 4G, Bluetooth etc.;
- **Servers and other computational systems** that use these data – such as: storage, analysis devices or dedicated software applications.

When all three of these components are found in the same system with the role to deliver services (and sometimes products), then we can really talk about added value created with the aim of developing citizens, the public and the private environment. A short example would be the smart devices that monitor the evolution/involution of a chronic disease in a patient by transmitting real-time data to doctors who may intervene if the situation requires so.

IoT applications and systems are organically developed – based on needs, but the impact they have on us depends on the degree of acceptance of new technologies by citizens, the public and the private sector [23].

The greatest risks that can arise from the extensive use of IoT come from the data security and cyber attacks area. However, the laws of the economy must be understood, namely that the most trustworthy products and services will continue to be procured by the beneficiaries – demand and supply are strongly connected. The Statistic Portal tells us that the IoT market has exceeded a trillion dollar at the end of 2017, forecasting an evolution of up to 1.7 trillion dollar at the end of 2019 [20].

2. Cities with senses

More and more cities in the world are experiencing the new dimension of sensor networks. Many are involved in pilot projects with the purpose of monitoring various activities in urban life, such as the level of noise or air pollution, parking management, health monitoring applications for persons suffering from chronic illnesses etc. **Thingful** is a search engine within this new dimension of the digital world. It contains indexes with the geographical positioning of all the fixed equipment connected in the world – a simple typing of a city's name can indicate on the map where different sensors are placed and what function they fullfil [21].

Thingful's goal is not just to provide a map of existing public or private equipments, but also to provide developers with solutions for smart cities to use these devices – of course, with the consent of the owners [21].

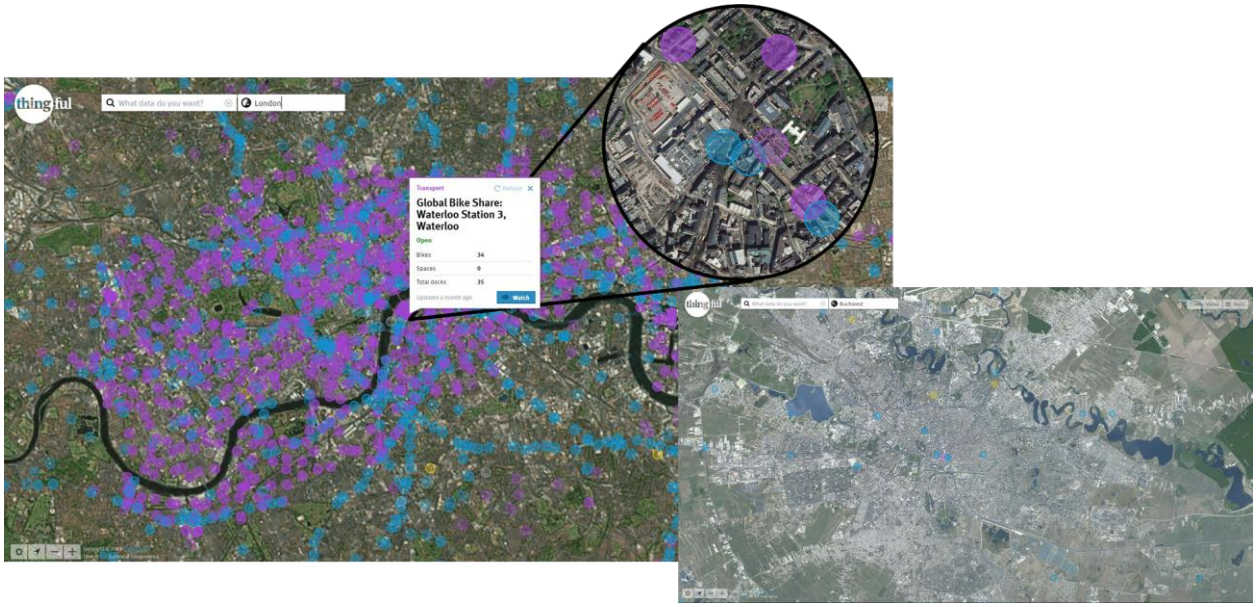

Figure 1: World of IoT in London, UK (left) and Bucharest, Romania (right) [21]

London has developed, with six partners, including Future Cities Catapult and Intel Collaborative Research Institute, the project **Sensing London**. Five living labs were built around the metropolis to collect data (obviously through sensors) about humidity, air quality, traffic and pedestrian activity. Subsequent analyzes directly help enrich the knowledge of how British capital residents use the infrastructure. At the same time, indirectly, these data are used as inputs in the health, environment and life comfort systems due to the statistical analyzes that can be carried out and thus the impact that a particular phenomenon can have in the area of interest researched can be predicted. From this point to developing new solutions (such as an application that would help asthmatic patients to travel through the city) or to developing new business models that allow the expansion of green spaces without major financial investment or even the justification for the development of new technological infrastructures is just one step [11].

The Christchurch city of New Zealand has developed, through a nonprofit organization, a similarly project called **Sensing City Trust**. The actors involved want to better understand how data gathered through sensors can help mayors to develop better public policies. After a devastating earthquake in 2011, a network of digital sensors was developed and installed as part of the city‘s physical infrastructure in order to gather information on air quality. In addition, 150 people registered in the public health system were recruited as chronic respiratory patients who were given a „smartinhaler“ which records where and when they are using medication to relieve symptoms. The data is then automatically transmitted via the smart phones the individuals owns, to a secured database, overlapping those that come from the sensors we mentioned and which were collected shortly before, and thus offered to decision makers for them to be able to develop the most effective public health policies. Supplementary to the initial purpose of the project, the information produced by the analyzes help doctors to improve their understanding of chronic lung diseases, thus managing to bring real benefits to patients by the fact that they can get treatment before reaching the hospital – in the event of an intervention, medical crews already know the condition of the patient, his/her needs and implicitly their response time is being reduced [15].

Chicago, in the United States, has developed a matrix of equipment – **Array of Things**. This is an interactive network of modular sensors that collects real-time data from the environment, from the physical infrastructure of the city, as well as those that target the behavior of citizens. The goal is

obviously to better understand the local urban environment and the impact it has on the lives of individuals living and working there – the most important elements for analyzes being those related to climate, air pollution and noise pollution. The data thus collected are open, meaning that are open to free use by residents, software developers, scientists or decision-makers. Citizens‘ behavior is detected through three different types of sensors: sound sensors, which collect data from the surrounding environment; infrared cameras oriented to car or pedestrian traffic areas and which are designed to record temperatures from the surface of fixed or in motion objects; and a wireless network that measures the number of nearby Bluetooth and Wi-Fi devices – it acts as a proxy for pedestrians in the area. Although questions can be raised that would concern the privacy area of citizens, the project guarantees that no personal or identification data are collected [1].

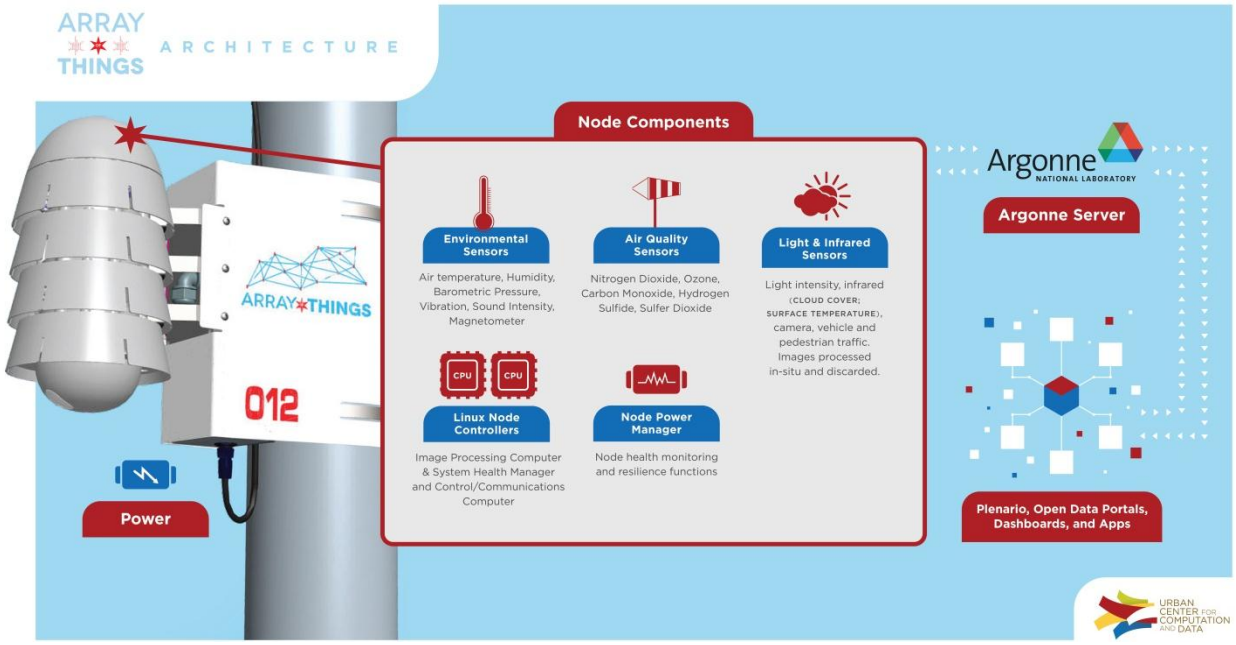

Figure 2: Architecture of the Array of Things system [1]

In Sibiu, Romania, was developed, thanks to the collaboration of „Lucian Blaga“ University of Sibiu with the University College of Southeast Norway, Norway, the project **A Mobile Platform for Environmental Monitoring** with the aim of producing an environmental map that provides all actors in the city‘s perimeter with information on air quality and noise pollution. The Faculty of Engineering within „Lucian Blaga“ University has developed hardware modules that can be placed on cars and which are meant to collect traffic data both when the car is in motion or in the parking areas, when the car is parked. The collected data is transmitted via a GSM module combined with a GPS module implemented on the equipment to a server that has the role of storing them and providing them for analysis to the actors involved. Two prototypes of sensors were realized, the last of them (and the most advanced) being able to collect both data such as the CO_2, NO_x level as well as the amount of suspended solid particles. The project is still in the pilot phase, with only 16 cars equipped with such modules in the city, being completely functional, a number of aproximately 100 units will be produced to be mounted on vehicles [4].

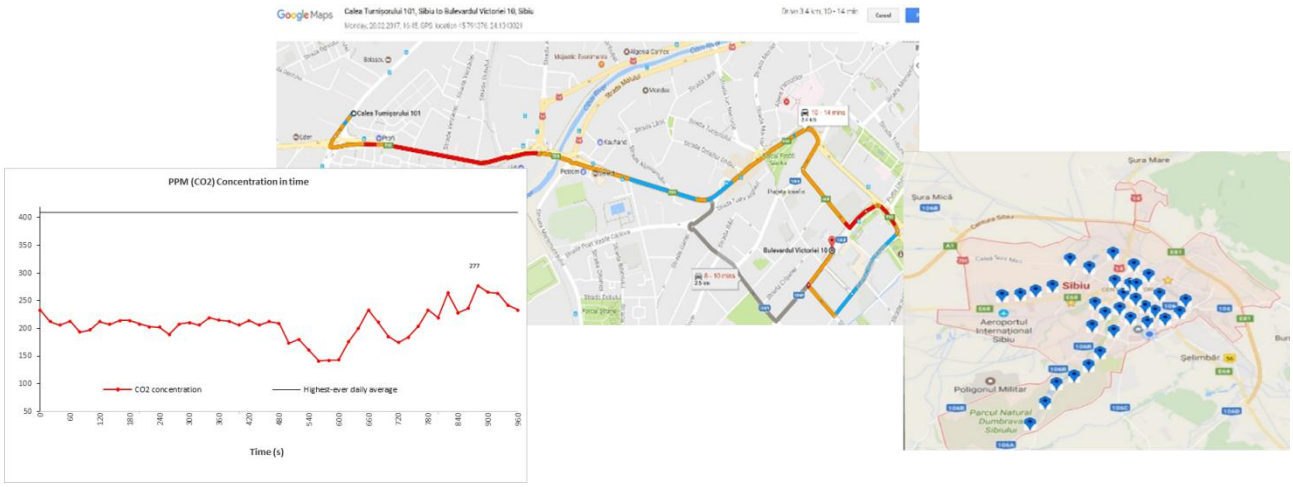

Figure 3: Data collected through mobile traffic platforms in Sibiu [9]

Therefore, we can see that IoT is spread all over the world and these various cities, mentioned above, have successfully implemented this concept and were given as examples in this paper in order to emphasize the ways in which IoT networks and services can contribute to develop smart cities, thus shaping even more the path to proving an answer to our research question, mentioned in the introductory section.

3. Some of the main risks of a connected city

IoT will bring innovations within smart cities, but with the creation of new innovations also arise difficult challenges. Some of the main and most common risks that the implementation of IoT can bring to smart cities are the ones mentioned below.

3.1. Cyber security

As our cities are becoming more and more saturated with sensors, they are becoming smarter and smarter [5]. However, we must also take into account citizens' degree of tolerance for the invasion of data collection equipment – as the number of equipment increases, the citizens feel more supervised [24].

The most common questions here are: (1) „Who produces and controls the equipment?", (2) „What do they measure?", and (3) „Who has access to the data?". All these questions are important and answers to them must be available to every citizen in a language that is as easy to understand as possible so that there is no confusion.

Other questions such as those related to the purpose of collecting data, the changes that will follow from these operations and the benefits of citizens, the public and the private sector are also important. Data storage management mechanisms (often software) are also commonly found in studies about IoT.

Many cities consider elements of security (obviously not only digital) and intimacy as key to sustainable and harmonious development. The level of trust and acceptance of the new by citizens is crucial in developing smart solutions. However, there is little written information on how citizens see these things.

The European Union, being concerned with this topic, has created the GDPR (General Data Protection Regulation) guide, which will start taking effect on May 25, 2018. Formaly known as EU 2016/679, this new regulation replaces Data Protection Directive 95/46/EC and has the aim of unifying the laws on data privacy from EU member states in order to protect and strengthen data privacy of European data issues. It also has the purpose to provide a uniform framework regarding the protection of personal data, thus strengthening the EU digital market [8].

Dan Gârlașu, from Oracle Romania, warned IT users that in the future smart cities may be more vulnerable to hackers than smart computers and smartphones are today [12].

With billions of interconnected devices all over the world, cyber security challenges are increasingly addressing also the IoT dimension of the digital world. Often the media poses on the front page of the newspapers titles that refer to hacking actions of different types of equipment. In the summer of 2015, the car producer Fiat recalled 1.4 million vehicles for software updates due to the risks of the machine safety being affected [3]. At the end of 2017, a clip posted on Youtube featured two hackers who stole a luxurious car by remotely cloning the door opening device and starting the vehicle [25]. Shortly after the event, CNN tech has produced the „Watch thieves steal car by hacking keyless tech" material explaining each action of the hackers [6].

Cesar Cerrudo, Chief Technology Officer of IOActive – one of the most prestigious digital security consultancy corporations, stated for The Independent in the UK that „a malicious hacker could use the information to manipulate traffic lights to cause jams and alter speed limits" [18].

***

This research area is particularly rich in topics. The European Union Agency for Network and Information Security (ENISA) launched in November 2017 some recommendations on IoT security in the context of critical information infrastructures [7]. Microsoft, Symantec, along with other leading companies in the cyber field regularly make reports on case studies accompanied by warnings and recommendations on this new dimension of the digital world: „Developing a City Strategy for Cyber Security" [14], „Transformational 'Smart Cities': Cyber Security and Resilience" [16]. Unfortunately, however, there is little information on how these recommendations are embedded in smart solutions implemented at city level.

Cyber security efforts tend to be focused on the role of local leaders in the development of smart cities and the IT&C embedded systems, although it is known that the development of such cities is much more complex, involving many partners in this process and as many technologies.

3.2. Temporary inoperability

IoT enthusiasm is often tempered by the connectivity problems that the equipment are faced with. The wireless ecosystem, though easy to understand, is hard to imagine. Due to the very large number of IoT uses, we cannot find a single standard – both in wireless technologies and in electricity consumption [17]. These two seemingly minor problems can cause major effects in the good functioning of an IoT system.

The technology of a smart city could be taken by surprise by the technological advances – new equipment is being developed, with new standards long before the old and already in motion ones are depreciated. Hence, many connectivity problems can arise between the equipment placed in the

wireless ecosystem of IoT. For example, we can imagine a smart city in which automated cars (without a driver) navigate by themselves on the city's streets. What happens when they pass through an area in which the sensors of the traffic lights are no longer compatible with theirs? Another question that arises is what happens when, due to network noise, communication between the vehicle and the traffic light system is slow or temporarily interrupted? Obviously, these questions must first find an unequivocal answer in order to be able to talk about a successful implementation of such a system [13]. In Figure 4 we can see the complexity of such a system and, practically, due to the large number of devices that need to communicate in a very short time, the risks associated to a small data flow disruption.

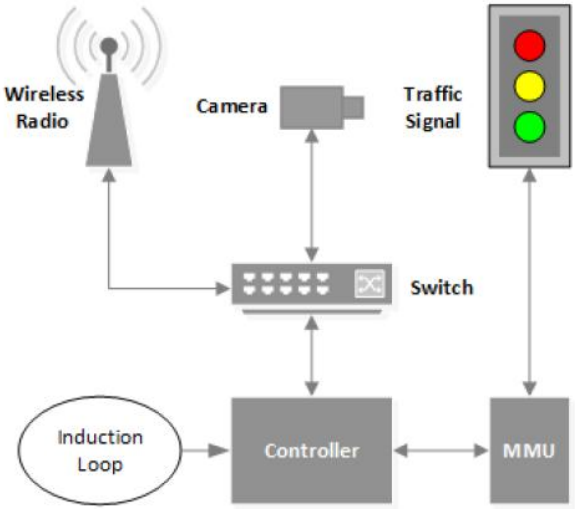

Figure 4: A typical traffic intersection [13]

All Internet users experienced situations where web pages were loading slower or when mobile calls were disrupted apparently for no reason. These situations can create frustration, but humans understand and know they can appear. But when we talk about electronic equipment, they cannot understand, and the effects of their misunderstanding can produce less pleasant effects for citizens or the environment.

If, in the case of the cyber security risks previously presented, the pressure was on the managers of a smart city, in the case of interoperability, the pressure tends to be put on the research environment, especially in the technological and academic areas. Only these can find viable solutions to such problems.

4. Conclusions

The dimension of IoT is not just a goal to be achieved – often mayors, hearing the concept but not understanding it in its depth, want to invest in IoT sensors and equipment for their cities – it is a remarkable symbiosis between society and technology. Many of those technologies that once represented the top ones are today viewed as part of everyone's life.

The parallel between IT and Internet innovations has led to a series of changes in the world economy such as the growth of the sector of products and services dedicated to informational economy. As Thomas Lauren Friedman (a New York Times journalist) said in his book „The world is flat: A brief history of the twenty-first century", written in 2005, „the Internet has flattened the

world, IT has first provoked and then increased the pace with which these changes have occurred, providing a platform for development" [10].

Of all the challenges of the electronic world, IoT is the newest and probably the biggest – due to the explosive evolution of the number of Internet-connected equipment. It must be well known, understood and managed. There is a hidden component in people's Internet, also known as Deep Web or Dark Web, where unknown operations are made and of which only the actors directly involved have a clue. Many of these operations are illegal. Why wouldn't the Internet of Things risk to have its own dark side? To minimize this risk, a proper education of all stakeholders is required, so that the responsibility for a successful system management will be implicit.

Taking all this information into account, we can observe that the response to this paper's research question is education regarding the concepts mentioned, which will be constituted as a solution to the problems that might occur in the implementation of IoT networks and services in order to contribute to the development of smart cities. Education can increase the capability and willingness of citizens, institutions of the public sector and also private companies to collaborate for implementing the best solutions for the communities. This is thus a subject to be developed in further research.

5. References

[1] ARRAY OF THINGS, https://arrayofthings.github.io/, accessed on 10.12.2017.

[2] ASTHON, K., That ‚Internet of Things' Thing, RFID Journal, http://www.rfidjournal.com/articles/view?4986, accessed on 10.12.2017 (2009).

[3] BBC NEWS, https://www.bbc.com/news/technology-33650491, accessed on 10.12.2017.

[4] BERNTZEN, L., JOHANNESSEN, M.R., FLOREA, A., Smart Cities: Challenges and a Sensor-based Solution, A research design for sensor-based smart city projects, International Journal on Advances in Intelligent Systems, http://www.iariajournals.org/intelligent_systems, Publisher: International Academy, Research and Industry Association (IARIA), volume 9, issue 3 & 4 (2016).

[5] BUSINESS INSIDER, How smart cities & IoT will change our communities, http://www.businessinsider.com/internet-of-things-smart-cities-2016-10, accessed on 10.12.2017 (2016).

[6] CNN TECH, Watch thieves steal car by hacking keyless tech, http://money.cnn.com/video/technology/2017/11/28/relay-box-car-theft.cnnmoney/index.html, accessed on 10.12.2017 (2017).

[7] ENISA, Baseline Security Recommendations for IoT, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot, accessed on 10.12.2017 (2017).

[8] EUGDPR, https://www.eugdpr.org/, accessed on 05.03.2018.

[9] FLOREA, A., BERTNTZEN, L., Green IT solutions for smart city sustainability, paper presented at the Smart Cities Conference, 5th edition, December 8, 2017, SNSPA, Bucharest, Romania (2017).

[10] FRIEDMAN, T.L., The World Is Flat: A Brief History of the Twenty-First Century, Farrar, Straus and Giroux, New York (2005).

[11] FUTURE CITIES CATAPULT, Sensing London, http://futurecities.catapult.org.uk/project/sensing-london/, accessed on 10.12.2017.

[12] GĂRLAȘU, D., Cyber Security Update on Threats and Trends, paper presented at the Smart Cities Conference, 4th edition, December 2016, SNSPA, Bucharest, Romania http://administratiepublica.eu/smartcitiesconference/2016/program.htm (2016).

[13] GHENA, B., BEYER, W., HILLAKER, A., PEVARNEK, J. and HALDERMAN, J. A., Green Lights Forever: Analyzing the Security of Traffic Infrastructure, Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT '14), August 2014 (2014).

[14] MICROSOFT CORPORATION, Developing a City Strategy for Cyber Security. A seven-step guide for local governments (2014).

[15] SENSING CITY, http://sensingcity.org/, accessed on 10.11.2017.

[16] SYMANTEC OFFICIAL BLOG, Transformational 'Smart Cities': Cyber Security and Resilience, https://www.symantec.com/connect/blogs/transformational-smart-cities-cyber-security-and-resilience, accessed on 10.11.2017 (2013).

[17] TEXAS INSTRUMENTS, Wireless connectivity for the, Internet of Things: One size does not fit all (2017).

[18] THE INDEPENDENT, Vulnerabilities in traffic light sensors could lead to crashes, researcher claims, http://www.independent.co.uk/life-style/gadgets-and-tech/news/traffic-light-hack-could-lead-to-road-chaos-claims-expert-9309936.html, accessed on 10.12.2017 (2014).

[19] THE STATISTIC PORTAL, Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, accessed on 05.03.2018 (2018).

[20] THE STATISTIC PORTAL, Size of the global Internet of Things (IoT) market from 2009 to 2019 (in billion U.S. dollars), https://www.statista.com/statistics/485136/global-internet-of-things-market-size/, accessed on 10.12.2017 (2017).

[21] THINGFUL, http://www.thingful.net/, accessed on 10.12.2017.

[22] UK RS ONLINE, https://uk.rs-online.com/web/generalDisplay.html?id=i/iot-internet-of-things, accessed on 10.11.2017.

[23] VRABIE, C., Elements of E-Government, Pro Universitaria Publishing House, Bucharest (2016).

[24] VRABIE, C., Your freedom starts where my privacy ends, Smart cities, Pro Universitaria Publishing House, Bucharest (2017).

[25] YouTube, https://www.youtube.com/watch?v=bR8RrmEizVg, accessed on 11.12.2017.