BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF FOREIGN LANGUAGES
ÚSTAV JAZYKŮ

NEGATIVE IMPACT OF SMART CITIES ON HUMAN SOCIETY
NEGATIVNÍ DOPADY SMART CITIES NA LIDSKOU SPOLEČNOST

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR — Daryna Sakharova
AUTOR PRÁCE

SUPERVISOR — Mgr. Pavel Sedláček
VEDOUCÍ PRÁCE

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Angličtina v elektrotechnice a informatice**
Ústav jazyků

Studentka: Daryna Sakharova ***ID:*** 185910
Ročník: 3 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Negativní dopady Smart Cities na lidskou společnost

POKYNY PRO VYPRACOVÁNÍ:

Lidská společnost je stále více koncentrována ve městech. Smart Cities jsou popisována jako východisko z krize přelidněných měst a o jejich pozitivním vlivu na životní prostředí a lidskou společnost byla napsána řada publikací. Úkolem této práce však je zaměřit se na negativní dopady Smart Cities na lidskou společnost a to z různých hledisek.

DOPORUČENÁ LITERATURA:

Townsend A. M.: Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia, Norton, W. W. & Company, Inc., 2014. ISBN 978-0-393-34978-8

Pool S.: The truth about smart cities: 'In the end, they will destroy democracy', The Guardian, 17th Dec 2014, <http://www.theguardian.com/cities/2014/dec/17/truth-smart-city-destroy-democracy-urban-thinkers-buzzphrase>

Institute for the Future: <http://www.iftf.org>

The City Fix <http://thecityfix.co

Termín zadání: 9.2.2018 ***Termín odevzdání:*** 25.5.2018

Vedoucí práce: Mgr. Pavel Sedláček
Konzultant:

doc. PhDr. Milena Krhutová, Ph.D.
předseda oborové rady

Abstract

The concept of Smart cities is predicted to be a future model of human dwelling. The main task of this work is to determine the role of Smart City's key components in order to estimate whether a smart technology always brings comfort and encompasses the area where people feel safe. In my bachelor thesis, I am going to present the concept of Smart City, by analysing and considering different definitions. In addition, it was important to include the chapter dedicated to the history of the term in order to trace its appearance and understand the reasons for the concept invention. Later in the thesis, I add key components and factors that influence the scientific perception of this term, in order to understand the concept Smart Cities and the way of its negative influence. The description of the main disadvantages of the Smart City realisation is presented in last two chapters of my work, where I provide the detailed description of the existing problems, representative examples, and reasons for their occurrence.

Key words

Smart city, Internet of things, Smart Grid, E-Government, Social Control, Cyber threat, Data collection.

Abstrakt

Koncept Smart Cities je považován za nový způsob lidského bydlení. Hlavním úkolem této práce je určení role klíčových komponentů Smart City, za účelem zhodnocení zda Smart technology přináší pohodlí a zahrnuje oblasti, kde se lidé cítí v bezpečí. Ve své bakalářské práci představuji koncept Smart City za pomoci analýzy a zvážením různých definicí. Pro objasnění konceptu a vysvětlení jeho užití bylo nutno zahrnout i kapitolu věnující se historii tohoto termínu a fenoménu. Aby čtenář snáze pochopil problematiku konceptu Smart Cities a jejich potenciálních negativních dopadů, bylo nutno zabývat se i faktory, které ovlivňují vědecké vnímání toho výrazu. Stanovením hlavních nevýhod jejich realizace se zabývají poslední dvě kapitoly mé práce. V nich poskytuji detailní popis stávajících problémů, uvádím příklady a objasňuji důvody pro jejich výskyt.

Klíčová slova

Smart City, Internet věcí, Inteligentní sítě, E-government, Sociální kontrola, Kybernetická hrozba, Shromažďování dat.

SAKHAROVA, D. *Negativní dopady Smart Cities na lidskou společnost.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2018. 44 s. Vedoucí bakalářské práce Mgr. Pavel Sedláček.

Declaration

I hereby declare that I have worked on this project independently, using the resources listed in the bibliography.

Prohlášení

Prohlašuji, že bakalářskou práci na téma *Negativní dopady Smart Cities na lidskou společnost* jsem vypracovala samostatně pod vedením vedoucího semestrální práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne…… ……

(podpis autora)

Acknowledgment

I would like to sincerely thank Mgr. Pavel Sedláček, for supervising my bachelor project and for his wise advice, which helped me in creating it.

Table of contents

1. Introduction

For the last decades, cities all around the world have been facing a great number of challenges. Cultural diversity, lack of safety, environmental pollution, restrict economic development and overpopulation are considered to be the major problems that are frequently being discussed and are currently remaining to be solved. Although taking into account all disadvantages that may affect the life of its citizens, cities have exploded to harbour more than half of the world's population. Comparing modern world with the situation at the dawn of the 20th century, when urban population contained merely 14 percent, it can be estimated that the world as we know it is heading to produce metropolitan nations (Florida, 2011). Urbanisation is enhancing with a great speed each year, and, in the future, our society is predicted to become predominantly urban. Moreover, globalisation has become an integral part of the modern world.

People have already accepted the fact that everyone is internationally connected. The significant invention of the Internet substantially contributes to the constant access to communication that definitely simplifies the people's life. Urban communities are increasingly requiring innovations in order to satisfy and simplify the life of its citizens. As a result, a Smart City is frequently described as the realisation of the physical world, where humans will be provided with computerised technology that will save their time, money and effort on the daily basis. As cities grow bigger, they are gradually being transformed into the nation's laboratories for innovations.

However, the Smart City concept is able to cause diverse effects on citizens' life. It can be assumed that these effects may also contain several disadvantages of dwelling in the technological environment. This work will be focusing on negative impacts that may be induced by the implementation of smart technologies.

At the beginning of my thesis, I introduced the basic definitions and the brief history of the Smart City concept including the initial aims that are followed by its realisation. Apart from that, in order to estimate whether this concept will contribute or, controversially, disrupt the city's infrastructure, it is important to analyse the main components that turn an urban environment into the smart one. I have introduced and described four major units that are the Internet of Things, E-Government, Smart grid, and Urban Living lab. In the next chapter of the bachelor thesis, I studied two significant challenges that may result in the numerous issues that may be seriously harmful to the life of city dwellers.

2. Definition

The term ‘city’ was always considered to be clear and explicit. According to Meriam-Webster, a city is an inhabited place of greater size, population, or importance than a town or village. Simultaneously, adjective ‘smart’ contains numerous meanings. ‘Smart’ is frequently thought to mean clever and intelligent. Referring to Meriam-Webster dictionary, another essential meaning emerges and asserts that ‘smart’ entails ‘operating by automation’. A great number of updated technological innovations require an important characteristic of ‘smart’ written next to the name of the product, solution, or, merely, idea. Nevertheless, the question arises why the term *Smart City* remains difficult to define and why it appears to be an ambiguous and vague project of inevitable future. In order to understand a concept of Smart City, it is necessary to deviate from the usual perception of the term ‘city’. In addition, it is crucial to clarify the word ‘smart’ in the context of cities.

From the pragmatic point of view, by being smart, the city is entailing strategic directions. From the marketing point of view, the term ‘smart’ is considered to be more user-friendly than ‘intellectual’ or ‘clever’. From the technological perspective, the smart technology is equating the problem-solving and multitasking technology.

The Smart City is described by a great number of institutions and enterprises that are developing the project of Smart Cities. For corporations like IBM, Cisco Systems, and Siemens AG, the technological elements are the key components of the Smart City conception. From their marketing materials, the Smart City appears to:

“… synchronise and analyse efforts among sectors and agencies as they happen, giving decision makers consolidated information that helps them anticipate, rather than just react to, problems.” (*IBM's description of a Smart City*) (as cited in Nesbitt, 2012).

“…the seamless integration of public and private services, delivered across a common network infrastructure, to individuals, governments, and businesses.” (*Cisco’s description of a SC*) (as cited in Elfrink, 2010, p. 2).

“Several decades from now cities will have countless autonomous, intelligently functioning IT systems that will have perfect knowledge of users’ habits and energy consumption, and provide optimum service. The goal of such a city is to optimally regulate and control resources by means of autonomous IT systems.” (*Siemens’ description of a SC*) (as cited in Greenfield, 2012, p. 12).

According to these descriptions, the Smart City can be regarded as the city that is supplied with a great number of information and communication technologies in order to enhance the operational efficiency and to improve the welfare of its citizens by processing and analysing the received information.

A.M. Townsend in his book "Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia" (2014, p. 97) claims that this is the concept where information technology is combined with infrastructure, architecture, everyday objects, and even human bodies to address social, economic, and environmental problems. Apart from technology, smart cities also require 'smart citizens' that are going to use the gained information about the environment where they dwell in order to make informed choices about their lifestyle options.

3. History

The humanity was aiming to achieve the symbiosis between Earth and Humankind throughout its existence. The world was constantly challenged by different problems such as environment, economy, security, education, etc. Digital age made people believe that technology can supply various solutions. Evidently, with technical improvements, people started to develop different methods of simplifying their life in the everyday prospect. Urban dwellings were not an exception and, for this reason, a question of optimising cities has arisen.

The first image of how a building might be integrated with the computers and smart technology was the project of "Generator" developed by Cedric Price during the 1970s. According to architectural historian Molly Steenson, the Generator was: "a set of building blocks, 150 stackable 12-foot cubes, all of which could be moved by a mobile crane as desired by users to support whatever activities they had in mind, whether public or private, serious or banal" (as cited in Townsend, 2014, p. 20). In order to realise this idea, he asked John and Julia Frazer, the architects who worked using computer technologies related to urbanism and architecture, to design a software that would rearrange the building automatically. They created the program called "perpetual architect". It would sense the layout of the modules and reassemble them overnight into a new pattern to provoke, delight, and otherwise stimulate the retreat-goers (Townsend, 2014, p. 21). As John Frazer **(**as mentioned in Interactive Architecture Lab, n.d.**)** wrote Price in their letter: "In the event of the site not being re-organized or changed for some time the computer starts generating unsolicited plans and improvements... In a sense the building can be described as being literally 'intelligent'", and he had also claimed that Generator "should have a mind of its own". Despite the fact that, the Generator had never been built, it was an essential project that the architect Royston Landau described as "a computerized leisure facility, which not only could be formed and reformed but, through its interaction with

users, could learn, remember and develop an intelligent awareness of their needs." (Townsend, 2014, p. 21).

Degtereva (2017) points out that during the 70s-80s of the 20th century, the next step to the automation world was made by designing the simple heating controls. However, the concept of Smart Cities started to be widely discussed since the 90s and was eventually extending itself. Primarily, the SC was regarded as the method for protecting the environment from the human detrimental effects.

In 2008, the active implementation period of the Smart Cities concept had begun. During this year, according to Townsend (2014, p. 6), our global world reached three historic thresholds: the urban population became equal to the rural population of the world; the number of Internet users who beamed their bandwidth down over the airwaves surpassed those who piped it in over a cable, and the invention of the Internet of Things. Samuel Palmisano, the CEO of IBM Corporation, gave a speech published in 2010 about the importance of creating a Smarter Planet. The aim of integrating technology into the aspect of everyday life fascinated a lot of corporations all around the world. According to J. Laartz and S. Lülf (2014) a study by the McKinsey Global Institute suggested that the world's 600 fastest growing cities would account for 60 percent of global economic growth between 2010 and 2025. The researchers claim that, in order to achieve and sustain the following level of growth, a great number of researchers are motivated by the Smart City concept.

Nowadays it is tangible how established cities all around the world are tending to be indicated as 'smart cities' in there marketing materials. For an instance, Stockholm, which claims to be one of the world's most connected cities, develops a fibre solution that is constantly contributing to making the city more attractive to businesses in general and the tech sector in particular (Kista Science City, 2014). Another example is Amsterdam Smart City (ASC) is an innovation platform that executes different projects dealing with smart city development and that is relating to such topics as infrastructure and technology, waste of energy and water resources, mobility, circular city, governance, education, and citizens' living. Apart from that, B. Cohen in his article dedicated to the top 10 smartest cities of North America claims that American cities, such as Seattle, Boston, or San Francisco, are ranking among the world's constantly refining cities. Another example that was considered to be the "quintessential smart city project" is the Centro deo Operacoes Preifetura do Rio de Janeiro (COR) is a constructed a Bond villain-style command centre in Rio de Janeiro, Brazil. It monitors weather, traffic flows and Live Streaming video cameras (Svetlik, 2015).

While, the majority of European and American examples of the smart cities development, in reality, appears to implement only separate elements using smart technology, Asian developers of smart cities introduce a concept of a completely new city that has to contain a vast number of modern and innovative technology. For an instance, India is currently preparing to develop 100 new smart cities across the country. One of the most famous examples is South Korean city Songdo that is advertised as the world's first smart city. This project was primarily launched in 2003 and the key idea lied in designing a genuine 'business center in North-East Asia' that was going to attract investments from all over the world and offering an unrivalled quality of living which would serve as a model to be exported (Mesmer, 2017).

However, evaluation of smart city success appears rather complicated by facing an increasing number of doubts and uncertainties. Respectively, it is essential to analyse the key components of the term and effects that they may entail.

4. Key components

4.1 Internet of Things

The Internet of Things (IoT) is "a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction" (Rouse, 2016). The key concept of the IoT term lies in the ability of things to sense various objects and collaborate with each other within one particular network. In terms of the IoT, 'things' contain a great number of embedded sensors, radiofrequency identifications (RFID) and technology that enable interaction with their internal states or external environment.

The term Internet of Things overlaps the description of the Smart Cities, due to the fact that both of the following terms contain the goal of handling the enormous amount of data in order to improve infrastructure, public utilities, and different client services. For this reason, it can be affirmed that Internet of things is the mandatory element forming the Smart City.

Since the beginning of the 20th century, the number of forecasts of the connected technologies that will make a huge impact on the urban life has considerably increased. The Cisco Internet Business Solutions Group (IBSG) estimates that the IoT is merely the point in time when the number of things connected to the internet exceeded the number of people (Evans, 2011, p. 2).

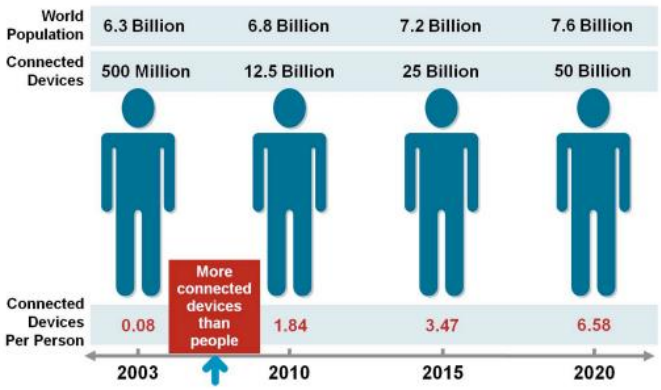

Figure 1. The Internet of Things was 'Born' between 2008 and 2009.

According to the infographic above, the IoT was established between 2008 and 2009 (see fig. 1). The updated stunning assessments claim that there will be 50 billion interconnected devices by 2020 (Nordrum, 2016). These devices are frequently believed to help to fill the gap between virtual and physical world.

The "Internet of Everything" concept presented by Cisco Corporation builds on the foundation of the "Internet of Things" by adding network intelligence that allows convergence, orchestration, and visibility across previously disparate systems. From a public sector leadership perspective, cities can be viewed as microcosms of the interconnected networks that create the IoE. The city leaders must understand how the components of the IoE — people, process, data, and things — play specific roles, and work together, to enable our future cities and communities (see fig. 2) (Mitchell et al., 2013, p. 2).

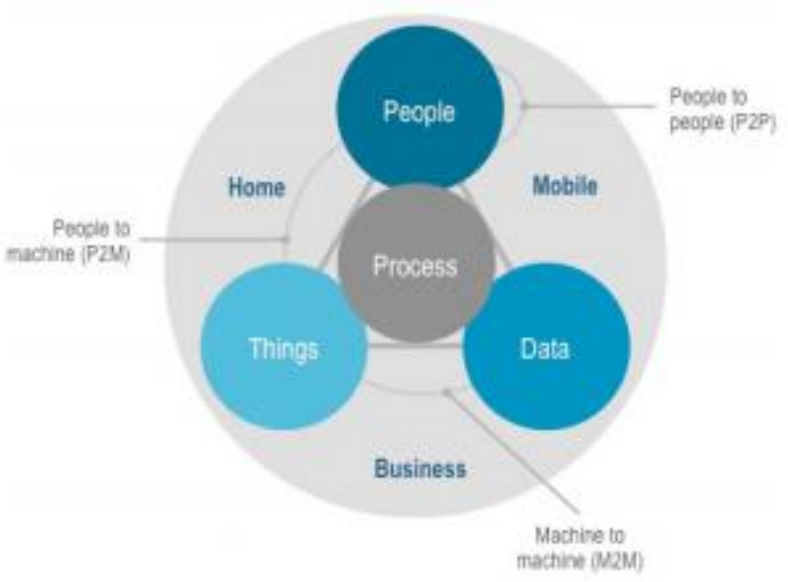

Figure 2. Internet of Everything.

The IoT applications contain an extensive number of conceptual solutions. These solutions can be separated into different categories based on the implicational and technological

domain. These categories include smart wearable, smart home, smart city, smart environment, smart enterprise (Perera, Liu, & Jayawardena, 2014). The detailed determination of these entities is presented in the following subchapters below.

4.1.1 Smart wearables

With an increasing number of connected devices, such as smart wearables and smartphones, humanity learns how to improve interaction with the digital architecture. Smart wearables represent the great diversity of technical devices that differ in their functions and applications and can be worn on different parts of a body (Perera, Liu, & Jayawardena, 2014). The recent example of smartwatch that resembles a wristwatch is capable of receiving calls and emails and can provide an access to online published information precisely corresponds to the following term. Due to the functionality of these devices, they are used for simplifying the life of its user and are frequently integrated into Smart Cities' projects. For an instance, the Utah state, USA piloted Google Glass containing a transit-tracking mobile app. The user of the wearable will receive an information about approaching bus or train, route map, and track vehicles in real time (Svetlik, 2015). Apart from that, SWs are commonly implemented as the health-monitoring devices by tracking the health status of patients in hospitals.

However, the smart wearable devices are often considered to entail pernicious effects. The question of citizens' privacy appeared with the experimentations of body-worn cameras that are used to document interactions between police and citizens (The Advantages and Disadvantages of Implementing Police Body Cameras and a Look at the Surrounding Current Legislative Activity, 2015).

4.1.2 Smart home

A Smart Home is a residence that is supplied with a great number of internet-connected devices, which allow the homeowners to remotely control their appliances and monitor lighting and heating systems. This can be beneficial for several reasons such as an increase in comfort and safety, technical adjustments that will satisfy the consumers' needs, and an efficiency improvement. This may introduce the relevant question of data privacy and security (Rouse, 2017).

4.1.3 Smart city

The term Smart City has been accurately described above. Nevertheless, it is essential to mention that Smart City relates to the Internet of Things conception due to its use of information and communication technology in order to find sustainable solutions for various growing problems. In order to accomplish various useful objectives, Smart cities are capturing,

analysing and using the Internet of Things and Machine to machine technologies. For an instance, sensors included in data sources could monitor air pollution, vehicle traffic flows, water levels, and energy consumption (Bernstein, 2015).

4.1.4 Smart environment

Mark Weiser defines a smart environment concept as "a physical world that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network." It will require air and water quality monitoring, natural disaster monitoring, and smart farming systems (Perera, Liu, & Jayawardena, 2014).

4.1.5 Smart enterprise

Smart enterprise solutions are designed to support infrastructure and to improve such industrial functionalities as management and connectivity. They include transportation and logistics, safety, energy and production and resources management concepts.

The above-mentioned components include a great number of promising capabilities. According to F. Mattern and C. Floerkemeier (n.d., p. 3), the IoT technologies can implement the following capabilities: communication, addressability, identification, sensing, actuation, embedded information processing, localization and user interfaces. People reckon that such urban problems as safety, traffic congestion, health care and quality of life can be solved by turning to IoT decisions. The eventual goal of the Internet-connected objects is to optimise an existing world to the extent where each element used by people in everyday life will be aware of the special preferences of the particular individual without his or hers explicit directives.

However, a great number of challenges appears with the development of connected things. In 2008, the national Intelligence council of USA, as mentioned in National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the Internet of Things, presented the Internet of Things concept as being “potentially disruptive” (2014, p. 4). Moreover, the NSTAC Report inferred that: “the rapid and massive connection of new devices brings with it risks, including new attack vectors, new vulnerabilities, and perhaps most concerning of all, the ability to use remote access to cause physical destruction” (2014, p. 3). For this reason, the main concerns of the IoT concept that include breach of privacy and over-reliance on technology are often considered to be the crucial reasons for postponing the IoT implementation. The possible lack of privacy raises another vital question of who is going to control the Internet of Things and where the collected IoT information is going to be stored. In addition, another crucial issue concerning the technology over-reliance underlines that currently

the system which is robust and fault-free does not exist. The continuing Internet dependence will entail a great devastating consequence in case of the system collapse (The Internet of Things, n.d.).

4.2 E-government

From the linguistic point of view, it can be assumed that the ‘e’ prefix, which appears next to the noun ‘government’, can demonstrate that the term ‘e-government’ relates to the internet or electronic technology. The Smart City concept frequently corresponds to the concept of E-government as its integral part. According to United Nations: E-government survey (2014, p. 55), the e-government can be determined as the employment of the Internet and the world-wide-web for delivering government information and services to the citizens.

The Global E-government Readiness Report made in 2004 (as described in UN E-government survey, 2014) determines e-government as the use of information and communication technology and its application by the government for the provision of information and public services to the people. Thereunder, in order to enable citizens to interact and to receive services from the federal, state or local governments twenty-four hours a day, seven days a week, the electronic government operations and its citizen engagement have to be supported by information technology, especially by the Internet (Palvia & Sharma, n.d., p. 2). The following interaction can be executed by obtaining information, making payments, or submitting applications via the World Wide Web. Sustainability, efficiency, and increase in the quality customer services are considered the main advantages of the e-government concept.

It is crucial to introduce the corresponding terms.

- E-governance

  It is frequently affirmed in different publications that the term ‘e-government’ composes the major subset of e-governance. The definition described by Keohane and Nye (2000) (as mentioned in Palvia & Sharma, n.d., p. 2) suggests that e-governance, unlike e-government, is not limited by the public sector but it implies administration and management on the private sector as well.

- M-government

  In recent years a term M-government (mobile-government) that complements E-government has become considerably discussed. The following term requires the use of wireless technologies in order to deliver government services (mGovernment, n.d.).

The question appears what does the e-government mean to the ‘e-citizens’ of the country that it is governing and whether it is possible to become one. The term ‘digital citizens’ sounds

abstruse and innovative, whereas, in reality, the current world of technical progress has reached the point where numerous people unconsciously appear to be digital citizens. Potentially, each member of society becomes a digital citizen after confirming an e-mail registration or using any other services that are available on the web.

The questions of surveillance, low rate of computer literacy in undeveloped countries, and insecurity of open data arise. In the majority of countries, the consumers of public services are the least likely to use the Internet due to the financial and age barriers. For these reasons, governments have to maintain all channels of communication open. That means that if services have to be provided online and offline, the savings may not match the cost of new technology (The good, the bad and the inevitable, 2008). Nowadays, only e-commerce is considered to be successfully implemented, while a limited number of countries has an option for its digital citizens to interact with government services by Internet and Technology use. The world-known example is E-Estonia that is aimed to be 'the most advanced digital society in the world'. It provides 99% of public services for its citizens that can be done digitally. Such services as i-Voting, e-Tax Board, e-Business, e-Banking, e-Ticket, e-School, University via internet, the e-Governance Academy are available for Estonians online. For example, Kristjan Kuurme in his speech called 'Estonia's e-Residency program' stated that "it takes only three minutes to declare taxes", or "it will take two hours to set up a company". Apart from that, one of the most recent concepts E-residency that is defined as transnational digital identity enables people all around the world to become a virtual resident of Estonia and use the offered services. It is significant to mention that by receiving a government-issued digital ID the person does not obtain a residency permit. Becoming an e-resident allow people to establish and run business in Estonia.

However, while the developers and founders of e-Estonia claim that "no-one – not hackers, not system administrators, and not even government itself – can manipulate the data and get away with that", the example of Russian cyberattack that happened in 2007 demonstrates the opposite. The following cyberattack resulted in cash machines and online banking services becoming out of action, and the inability of email communication of government employees. Apart from that, newspapers and broadcasters were completely unable to deliver the news. The government was later informed that these issues were the external cyberattack. The above-mentioned example illustrates how disruptive can be the lack of cybersecurity (Lufkin, 2017).

4.3 Smart Grid

The majority of people living in modern society has become used to have constant excess to electric power. As determined by the U.S. Department of Energy (n.d.), the grid that refers to 'electric grid' is a system that distributes the electric power from power plants to consumers. However, it has been frequently estimated that the current power grid has to be renewed to the extent of becoming automated and being able to handle a great amount of digital and computerised equipment. Optimized management of energy resources appears to be one of the main innovative solutions that address social, economic and environmental effects. The Smart Grid has to consist of a great number of new technologies, controls, computers, and sensors that will work with electric grid in order to respond digitally to consumers' electric demands. For this reason, the Smart Grid has to include 'two-way' network of communication enabling consumers, operators and automated devices to track energy use data in real-time (Wichmann, 2014). The Smart Grid is a concept of automated, widely distributed energy delivery network that will be capable of monitoring different devices.

- Smart meter

  The definite advantage of the smart grid technology is that consumers will be able to monitor their energy consumption. Nowadays, the special Smart meter which is the significant example of the device used in the United Kingdom measures gas and electricity consumption and displays this on the in-home display (What is a Smart Meter?, n.d.). This device enables two-way communication between the meter and the central system. However, it is complicated to measure the accuracy of measuring device, and it is impossible to protect collected data (Sunshine, 2018).

Implementing Smart Grid technology causes considerable concerns that are dealing with increasing risk of security breach. Improved capabilities of the conventional power network will make the grid more complex that will increase privacy vulnerability. In 2004, the head of the National Security Agency (NSA) stated that there is an existing possibility of such critical infrastructure as electric power grid being hacked potentially leading to "catastrophic failures" of this system (Hoskinson, 2014). Apart from that, network monitoring and managing will become extremely complicated. Marie Hattar, vice president of marketing in Cisco's Network Systems Solutions group (as cited in Morsella, 2009) stated that "Our expectation is that this network will be 100 or 1,000 times larger than the Internet." For this reason, the realisation of smart grid causes a vast number of serious doubts that, for today, remain to exist without workable solutions.

4.4 Urban Living Lab

Living labs are defined as "user-centered, open innovation ecosystems based on a systematic user co-creation approach in public-private-people partnerships, integrating research and innovation processes in real life communities and settings" (Robles et al., 2013). In the practical point of view, Dr. Kes McCormick determines the Living Labs as "sites in cities used to design, test and learn from social and technical innovation in real time and in integrated ways" (Bulkeley et al., 2017, p. 1).

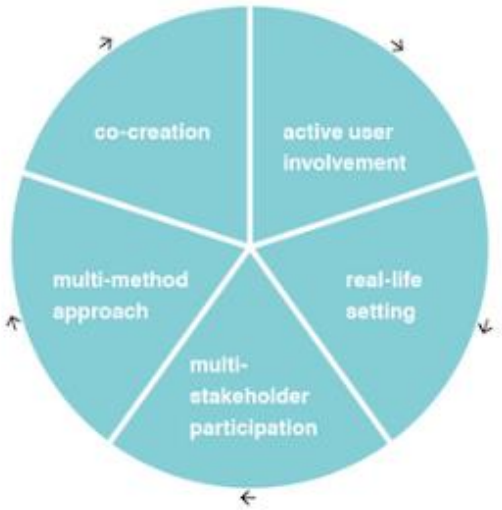

Figure 3. Common elements in Living Labs.

The goal of the living labs is to achieve the urban sustainability by the development of new products that can appear to be technology, service, process or a system. The research process has to be integrated into the life of city dwellers in order to estimate the most efficient way of city planning by studying the citizens' behaviour preferences. For this reason, the following concept includes the citizens' active engagement in innovation and development.

Nowadays, the Living Lab is frequently used by the urban-planning developers in Smart City projects and is regularly referred to as City Labs. These real-life applications of various social innovations that can be implemented in urban settings or local governments are aiming to study and face numerous urban challenges. Due to the wide variety of city challenges, it is essential that policymakers, researchers, and lab practitioners exchange ideas and form experiences in terms of structure, processes of co-creation and engaging of participants in urban lab initiatives (Höflehner & Zimmermann, 2016, p. 11).

However, G. Nesti (2017) presents different drawbacks related to these innovative urban services. First of all, the ULLs solutions are considered to be 'prototypes' in the majority of cases that do not require their implementation in the long-term policies, due to their experimental nature. Apart from that, the management of ULLs can be very challenging for the

public administration because of its requirements of the traditional project management with pre-determined resources instead of innovative mind-set.

To summarise the Chapter 4, it can be inferred that by analysing the key concepts that are frequently equated with an integral part of the Smart City term, the following possible issues can be distinguished:

- Social control caused by the lack of privacy;

- Cybersecurity issues;

- Vulnerabilities of the system and the possibility of different errors;

- Introduction of digital inequality;

- Psychological issues caused by an excess of technology usage.

The next two chapters will be focused exclusively on negative impacts of the technologically based cities, namely on the problems of social control, vulnerabilities that involve possible cyber threats, and mistakes of interconnected devices.

5. Social Control as a negative impact of Smart Cities

Due to the fact that technology is frequently believed to enhance and simplify each aspect of human lives, the modern world is becoming more and more computerised. People are no longer astonished by the constant presence of digital devices.

The enhancement of urban technological networks is frequently entailing various comprehensive methods of data collection. Frank Pasquale, a professor of Law at University of Maryland's Francis King Carey School of Law, and Jathan Sadowski, a PhD candidate in the "Human and Social Dimensions of Science and Technology", in their article “A spectrum of control: a social theory of the smart city” list an array of existing technical systems that are based on gathering information. For an instance, the smart wearable called the health wristband is collecting and analysing somatic data in order to clarify particular features of an individual. Another essential example is the location-tracking sensor that is continuously capturing and registering geospatial coordinates. Evidently, Smart cities will necessarily include a considerable number of these and co-related systems.

Nowadays, with the continuing modernisation of urban dwellings, cities are more and more depicted as the leverage of technology. Being rapidly filled with ‘smart’ technologies, cities are transformed into the platform for the ‘Internet of Things’ that is defined as the network of interrelated items, such as sensors and actuators, which collect and exchange information

between each other. Collecting and analysing Smart Data is one of the key tasks that have to be performed in order to maintain the sustainability of Smart City existence.

The Smart Cities are frequently advertised as the elaborate form of human inhabitancy where intricate sensors, cameras, and wireless devices are reporting data in real time and by that are allowing officials to rapidly respond to unpredicted circumstances, develop the sufficient energy use, prevent traffic jams or be aware in advance of environmental threats. However, the question arises whether the implementation of the above-mentioned strategies is going to lead to the 'steering' (manipulation and threatening) through technology.

5.1 Privacy concerns (Data collection)

It is frequently estimated that cities are gradually being transformed into the eventual setup for surveillance. The countless number of systems that are capable of recording, identifying, influencing and controlling people's behaviour and movements can be the quintessential example of the society being closely monitored (Townsend, 2014, p. 15). The continuous presence of these tools has become intangible for human perception. The size of the street cameras is being constantly reduced, thereby nearly eliminating the possibility of noticing them in the public places. The majority of people is not aware of the extent of their daily interaction with these devices. With street cameras and other types of face recognition technology, the person's face is enrolled into a giant network, regardless of his or her will to be enrolled (Sadowski & Pasquale, 2015). The question arises whether it denotes the fact that the possibility of moving undetected through the city supplemented with smart technology is significantly reduced.

In the interview made by J.L. Hester (2017), Lee Tien, who is a senior staff attorney at the Electronic Frontier Foundation, stated that people are not aware of all their 'traces' that are out in the world. He also considers the following data trails such as parking meters, streetlight cameras, automatic license plate readers, and binary DNA that is constantly being sloughed. According to Tien, trying to abolish these huge quantities of data streams would be impossible. As the technology is being rapidly evolved, it is causing much more issues for individuals to keep their data private and safe. As Jane Jacobs wrote in 1961: "This ubiquitous surveillance threatens to upset the balance of power between city governments and city residents, and to destroy the sense of privacy and urban anonymity that has defined urban life over the past century." (as cited in Finch & Tene, 2016, p. 3).

However, the extent to which people perceive their privacy and confidentiality of their personal lives appears to be a highly controversial subject. The world experiences the notable lack of appropriate secure behaviour, whereas the modern society expresses mounting concerns

about privacy matters. As mentioned in the article 'Privacy concerns in Smart cities' (2016), the most used pin code is 1234. Apart from this, internet users choose one password for multiple accounts. In addition, the personal information is widely shared on the endless variety of social media platforms. Young and Quan-Haase (2013) determine this type of social attitude as so-called "Privacy paradox" (Zoonen, 2016, p. 3).

People are conspicuously neglecting their responsibility for the data they share. They frequently rely on the fact that somebody else will ensure them with their confidentiality. The recent example of data capture negligence is the conflict that happened between the data analytic firm called 'Cambridge Analytica' and Facebook. According to a report from the New York Times (2018), this analytical firm harvested user data of more than 50 million people from their Facebook profiles without their permission. It is estimated to be one of the largest data leaks in the social network history. As cited in the New York Times magazine: "The breach allowed the company to exploit the private social media activity of a huge swath of the American electorate, developing techniques that underpinned its work on President Trump's campaign in 2016." After publishing this article, Facebook and Marc Zuckerberg, who claims that there was no leak due to the fact that users agreed for their data to be used, received a huge amount of criticism from the lawmakers and Facebook users (Rosenberg, Confessore, & Cadwalladr, 2018).

For this reason, people need to be aware of the importance of data security and confidentiality. In Smart Cities concepts, the privacy concerns should be solved by the safe storage, security from the functionless usage, and certain restrictions in data erasure.

5.2 Biometric monitoring

The Smart City monitoring will be a complicated task of creating a coherent and structured information about its citizens. The gathered data will be undoubtedly distinguished according to purpose, size, complexity of the structure, etc. As the Internet of things is introduced as one of the key concepts, the task is not only to collect, but also to share this diversity of information among all data systems.

For an instance, in Songdo, which, so far, appears to be the most approximate realisation of the Smart City initiative, all major information systems (residential, medical, business, governmental, etc.) share collected data. Everything that is done digitally is tracked by local governments. Each aspect of public service is digitalized and made available to the citizens of Songdo (Keeton, 2015). Apart from that, the houses, streets and office buildings contain the inbuilt computers (O'connell, 2005).

Songdo is the ubiquitous city where 500 cameras are used to regulate the traffic or detect suspicious behaviour (Mesmer, 2017). An advanced communication system allows users to contact the municipal administration from their TV screens, wireless access to citizen's digital content and property, let alone the availability of videoconferencing calls between house neighbours (Neidhart, 2018; O'connell, 2005). Additionally, everything is monitored in a control centre with a gigantic data screen (Neidhart, 2018). The initial question of the possibility of unwitnessed existence seems to be completely irrelevant after above-mentioned Smart Cities techniques implemented in Songdo.

According to Mr. Townsend, who is the author of the book "Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia", the reason for employing these smart strategies that were originally developed in U.S. is that: "there are fewer social and regulatory obstacles to implementing them in Korea". He has stated that Korea holds a historical expectation of less privacy compared to the western democracies, where this kind of implementation could hardly be accepted. In Asia that contains a great number of technologically oriented countries, the question of privacy can take the second place, due to the fact that innovative technology can attract foreign investment (O'connell, 2005). The idea of the implementation of ubiquitous technology is highly controversial in the West, where privacy issue is raised much more frequently than in the Eastern countries.

It is assumed that in the foreseeable future similar technologies will be introduced in Seoul, and will also be practiced in the construction of new megacities and, partially, in existing European cities (Econet, n.d.). In contrast to Songdo, Smart Cities are not necessarily built from the scratch, but existing cities can conceive the projects of "shock therapy" (or "smart shock") methods. Jathan Sadowski and Frank Pasquale describe 'smart shock' technique as the process that contains a rapid, large-scale integration of 'smart' ideas, policies and devices into an existing city landscape. Korean cities are not the only representative example of the surveillance technology and connectivity realisation.

A popular trend of connecting, processing and storing large amounts of information lies in data centres development. These centres are used in order to facilitate the accessibility by using innovative analytics and supercomputing (Lerman, 2018). The number of cities that aim to realise the customized and integrated data sources viewed on the unified display is increasing.

A great example of the urban command centre is Brazilian Centro de Operações Prefeitura do Rio de Janeiro (COR) that has been initially built as the rain prediction tool and has been gradually transferred into the constant surveillance panel (see Fig. 4). This data analytics centre acquires data streams from thirty agencies, including traffic and public

transport, municipal and utility services, emergency services, weather feeds, and information sent in by employees and the public via phone, Internet, and radio (Kitchin, 2014).

Figure 4. Centro de Operações Prefeitura do Rio de Janeiro.

Global companies like Google, Amazon, IBM, and Cisco broadly conceive numerous projects that are dealing with the city data centres (Lerman, 2018). These data integration and control centres are implemented in order to create the world where each aspect of a citizen's life is captured and feasibly never forgotten (Kitchin, 2014).

However, in order to execute the streaming of camera data, data centers are not necessarily required. The causes for CCTV implementation are commonly overlapping one another in numerous projects all around the world.

The security industry report made by the British Security Industry Authority (BSIA) outlined that Britain has one CCTV camera for every fourteen people (Barrett, 2013). It has been recently estimated in the article "How many CCTV cameras in London?" (n.d.) that there are 500,000 CCTV cameras dotted around London. It is also stated that an individual living in London is daily filmed by street camera approximately 300 times per one day. Nick Pickles, director of the privacy campaign Big Brother Watch, affirmed that the above-mentioned report can denote the fact that our society has gradually generated the total surveillance culture. Apart from that, he claimed that due to the potential number of five million CCTV cameras installed across Britain, citizens are monitored in the way that does not correspond to the ideas of the healthy democratic society (Barrett, 2013).

Another significant example denoting the overestimated expectations that were soaring around surveillance cameras installation appeared in the Netherlands. In 2013, in Amstelveen,

which is the suburban part of Amsterdam, another CCTR (Central Camera Surveillance Room) was opened. In order to attain the solution of drug-related nuisance and to increase safety by prompt crime detection, live images that are taken from an approximate number of 200 surveillance cameras installed in various parts of the city are constantly monitored by specially trained policemen. However, in the project report of the surveillance cameras effectiveness, Winkel (2011) stated that its realisation did not increase the level of subjective safety within the citizens.

The modern world tries to adjust itself to the increasing technology usage regardless the social concerns. For an instance, the current situation can be compared with the cell phone usage. When cell phones had merely started to appear on the market people were not obliged to have one. Nevertheless, nowadays, when almost everyone uses it, it is complicated for an individual not to conduct himself with this device (Sadowski & Pasquale, 2015).

There is an existing parallel between the smartphones and Smart Cities applications that are implemented in order to improve city management services. Although it is true that people can still voluntarily choose not to use their cell phones, it is almost impossible to voluntarily avoid being monitored. An urban government of Smart Cities leaves its residents with no alternatives but to follow services based on smart technology. Moreover, due to the wide array of sensors and other types of monitoring technologies, even those city dwellers who prefer privacy-aware services will be forced to give the consent for its implementation (Finch & Tene, 2016, p.17).

Evidently, the ambiguity whether the Smart City can be necessarily equated to the better one arises. It can be reasonably inferred that the constant data collection within city environment can turn it into electronic panopticon where each member of the society is continuously watched (Finch & Tene, 2016, p.4).

5.3 Policing technologies

The CCTV, databases and modern predictive software are considered to be the new surveillance technologies that allow police to increase the fields of vision and to collect evidence (Brakel & Hert, 2011-3, p. 9). In order to guarantee the safety of the Smart City citizens, streets are going to be constantly watched in real time. Different urban areas will be monitored with the help of embedded sensors and flying drones. During the current years, this technique has already been employed in various kinds of ways.

One of the most recent novelties is PredPol software developed by American Predictive Policing Company. The main aim is not only to detect crime but also to prevent it from

happening and to provide safety to city communities. In order to complete this task, gathered data must be analysed so that possible future crime locations and time are anticipated.

The concept is frequently advertised as the tool for improving law-enforcement. In the interview with the Economist magazine, Mark Johnson, the internet and society correspondent, stated that, currently, in the majority of cases, the predictions based on location data are preventing the crime from happening. However, he had also mentioned other studies that are dealing with the determination of the individuals who are more likely to break down the law. These sorts of assessments can reach an extent when people who have not previously committed any type of crimes can be as well considered to be the potential future criminals (The Economist, 2013).

In order to complete the task, a great amount of information that may also contain pieces of private information of the urban dwellers must be analysed. Johnson affirmed that information published in social media is likely to be collected in order to produce risk assessments of individuals who are unknown to the police. Although the above-mentioned strategy is frequently believed to be developed to provide the 'pre-criminals' with various benefits in order to prevent them from becoming actual ones, there is a serious possibility that these people can be arrested for the risk of committing a crime.

Another essential technical innovation is actively encouraged. The concept lies in the employment of 'smart' household appliances that will help the authorities to investigate causes of the incident. Information is going to be extracted from the embedded sensors and cameras of such household devices as washing machine, refrigerator, TV, etc. (MAKiPI, 2015). The surveillance and data collection technologies are equating our world with George Orwell's "Nineteen Eighty-Four" society. The question arises whether safety is actually more important than privacy.

The further crucial example takes place in Ohio, USA, the company called Persistent Surveillance systems has launched a civilian aircraft that allows monitoring cities from the air. Ross McNutt, the company's owner compares the product with "a live version of Google Earth, only with TiVo capabilities" (Campbell-Dollaghan, 2014). Sadowski and Pasquale describe the technology as letting police record, rewind, and zoom aerial video so they can track the movements of specific vehicles and people within the city. It is currently still not possible to identify people by face. However, with the parallel implementation of the street or red light cameras and other video sources, suspects can be easily distinguished (Campbell-Dollaghan, 2014).

Technology keeps being rapidly improved and developed. There is no factual guarantee that in the short time the above-mentioned trekking aircraft will be supplemented with a certain

allowance of ammunition. Moreover, the approximate concept that appears to be the first riot-control drone has already been introduced by the South African company called Desert Wolf. Carrying the catchy name *The Skunk* it is equipped with four paintball guns that can be loaded with dye marker balls, pepper spray balls or solid plastic balls. During strikes or demonstrations, The Skunk operator is able to use implemented paintball guns in order to disperse people in the crowd (Doctorow, 2014). The question how the police and security forces will evaluate the situation to the extent when this flying weapon can be involved remains unanswered.

Evidently, the predictive policing techniques can be implemented not only in the city with Smart initiatives but can also become a separate feature of any urban environment. However, it is a complement to the numerous Smart Cities projects where it is strongly advocated.

5.4 'Smart' cities or 'Data' cities?

A world-known phrase "He who owns the information, owns the world" contains the reason why local governments are attracted to the implementation of the smart tools to the cities infrastructure. The great number of concepts like Urban Living Labs that are all based on information gathering are constantly being developed and introduced. They are frequently advertised as the effective solution that will help to attain the real smart city planning and maintenance.

Taylor and Richter (2015) affirm that the technological developments that are currently happening all around the world indicate that data is a key to the rise of Smart Cities (Zoonen, 2016, p. 2). Evidently, the massive amount of information has to be obtained and handled in order to enable the comprehensive monitoring and city management and to maintain air and water quality, control the sufficient energy usage and neighbourhood sentiment. For an instance, Powell (2014) uses the term 'data cities' referring to 'smart technologies' that simultaneously collect an enormous mass of data (Zoonen, 2016, p. 2). Cities all around the world are rapidly transformed into data based cities. For an instance, the table below (see Tab.1) that contains the Rotterdam data landscape can perfectly illustrate the diversity of collected data that is based on the Urban Big Data Lab projects and interactions (Zoonen, 2016, p. 3).

Sector	Domain	Kind of Data	Example of application
Infrastructure	Transport and asset management, built environment	Monitoring data, registration data, geo data	Traffic and congestion patterns, real time dashboards
Sustainability	Energy usage, water, environment, weather	Sensor and monitoring data, civic measuring data	Air quality monitoring and pollution warnings
Health	Health, quality of life, well-being, life expectancy	Health data, survey data, lifelogging	Location specific noise levels and social or health problems in specific neighbourhoods
Cohesion	Education, social capital, migration, neighbourhoods, housing, crime	Survey data, civic and community web presence data	School quality in specific neighbourhoods
Commerce	Business opportunities, marketing, location based services	Social media, open government data	Investment maps or attracting new business
Experience	Events, leisure, nightlife, tourism, heritage	Social media data, archive data, sensor data	Real time social media analytics for crowd control

Table 1. City data landscape.

Form the Table 1, it is possible to notice that gathered data relates to almost every aspect of a modern citizen. It contains comprehensive information that is dealing with geographic locations, health status, data referring to civic duties, social media sharing, etc.

Due to the fact that data is rapidly diversifying, multiple facilities combining analytic techniques are required in order to handle this sorts of information (Zoonen, 2016, p. 2). According to Albert Meijer, who is the professor at Utrecht University, and Manuel Pedro Rodriguez Bolívar, who is the researcher at Granada University, there is generally a lack of supervision of this diversity of data streams within the big cities. The data emerges from numerous sources, including government departments, private and public stakeholders and private individuals, but is simultaneously gathered, stored and operated without any central coordination or collaboration (Zoonen, 2016, p. 2). Adam Greenfield, the author of the book called “Against the Smart Cities”, stated that such crucial decisions referring to “how, when and where to collect data”, reliable means of its interpretation and labelling have not been hitherto made (Newitz, 2014). It can be inferred that crucial concern of data organisation remains under an arbitrary solution, while it is regarded as the key factor of the provision of Smart City management.

Another important issue is dealing with the collected data quantification and retention. The ubiquitous surveillance and data capture have, presumably, become allowable to the modern citizens. The ownership of all data collected by smart tools enables to control society either for public benefits or for private gain. According to Kitchin (2014), when the types of sensitive information are proceeded by local governments, it is vitally important to balance the benefits of data analytics with individual rights of confidentiality.

However, nowadays there is no empirical evidence that could confirm the fact that the certain limit has been established in order to control governmental misuse of data.

There are policies that strongly advocate the Big Data collection by claiming that the gathered data is either almost never be browsed, and even in case it is, unless the browsed person is a criminal, it is completely secure (Ball, 2013). Nevertheless, each obtained piece of private information is potentially able to reveal confidential details about the person's life.

The fact that the National Security Agency of USA (NSA) in case of need can examine an archive of collected information about each citizen has already been ascertained. Edward Snowden who is a former National Security Agency subcontractor that had leaked highly secret details dealing with NSA phone surveillance activities (A&E Television Networks, 2018) and by that posed the questions concerning what information is being collected, what is allowed under the law, and how much is being done. By virtue of his leaks, the fact that NSA collects approximately 200bn pieces of intelligence from computer and phone networks every month was promulgated (Ball, 2013).

Surveillance and information gathering are frequently regarded to be two major innocuous strategies focusing on the prevention of terroristic attacks. According to Snowden, there is no evidence that programs that are based on mass surveillance techniques are contributing to the elimination of terrorist attacks. He claims that the true reason why these measures remain to be necessarily used lies in other governmental interests of spying. These surveillance methods contribute to the initial governmental purpose to attain more power in executing economic espionage, diplomatic manipulation, and political influence. (Knobbe & Schindler, 2017).

Catherine Crump in her talk for TED conference called '*The small and surprisingly dangerous detail the police track about you*' provides a great number of examples when the police departments collect various types of data about city dwellers. She emphatically asserts the fact that government is able to make a detailed portrait of each citizen based on the information that used to be private. She describes the Automatic License Plate Reader (ALPR), which is the high-speed, computer-controlled camera system that is mounted on street poles, streetlights, highway overpasses, mobile trailers, or attached to police cars

(Electronic Frontier Foundation, n.d.). ALPR indiscriminately captures images of each passing vehicle in order to record the license plate number. Apart from that, the data occasionally includes the photo of the driver and passengers. This device gathers information relating to location, date and exact time (Electronic Frontier Foundation, n.d.). The central services, which are commonly the local police departments, receive gathered data and check whether the driver is potentially wanted for committing an offence (TED). However, these records are increasingly being kept for an extended period of time (frequently more than 5 years) and include data of each tracked vehicle, despite the fact that the majority of collected and stored license plate data relates to people that have not preliminarily been accused of a crime (Electronic Frontier Foundation, n.d.). Ms. Crump has appended that this can denote the collection of mass quantities of data about where citizens have gone before. For an instance, she mentioned Mike Katz-Lacabe who requested the information that police department had previously collected about him by generating the data from the plate reader. As the result, the data which was presented to him contained a tremendous number of photos about the daily life of Mr. Katz-Lacabe.

Recently, technology has managed to deeply embed itself into urban lives. Apparently, Smart cities are heading to the realisation of constant surveillance and control of personal lives. Even though the majority of people assert that they have nothing to fear, due to the fact that they have nothing to hide, still, not everyone is ready for the publicity. Intelligent agencies and police departments that execute the mass data collection store everything in case it can become useful one day (Ball, 2013).

As Ms. Crump stated at the end of her speech that the aggregate data stored for an extended or indefinite period of time becomes more invasive and revealing, and causes the possibility of misuse and data breach. This leads to an increasing threat of civil liberty. In order to secure data against the malignant use, it is vitally important to develop strict limits on the amount and terms of storage and to introduce specific laws determining who will be able to access and manage the data. Technologies can only be positively evolved if the data of the innocent city dwellers is legitimately used by ensuring their confidentiality, as it is one of the fundamental human rights, which is mandatory to maintain human existence within dignity and respect.

6. Vulnerability of the System

The rapid growth of urbanization is causing a vast number of growing problems such as inadequate infrastructures, high population density, increase in crime rate, frequent traffic congestion, etc. (Okorie, 2015). The development and implementation of smart technologies

are considered an effective solution entailing the prompt enhancement of citizens' life. Internet of things is one of the key strategies that is currently inserted into the recent projects dealing with the city adjustment. Multiple cities including Amsterdam, Barcelona, Santa Cruz and Stockholm are already in the process of engaging a network of interconnected sensors inside the city called a "Smart Grid" used for the electricity supply.

However, every new technology introduces the new possible challenges. Due to the fact that the deepening integration of technologies with new or already existing urban landscapes is an indispensable condition for the Smart Cities implementation (Reys, 2016, p. 1), it is crucially important to distinguish the new forms of risks and vulnerabilities that are likely to augment.

6.1 Errors caused by the machine-to-machine interaction (M2M)

Inevitably, Smart cities concept implies numerous machine-to-machine interactions. The M2M communication overlaps the Internet of things concept as it contains a large number of intelligent devices connected by wired/wireless links, which cooperate with each other without direct human intervention (Verma et al., 2016, p. 1). It is implemented due to the large amounts of data that has to be processed in order to execute efficient decision making at the speed required by the system (e.g. energy grid).

The absence of human interaction can cause the system to commit *the cascading error*. This can be defined as the small, unnoticed mistake that was transmitted among the interconnected entities and is eventually transformed into systematic risk. Even though the initial scale of such errors is relatively small, in case of their occurrence in the huge industrial zones, they can gradually cause consequences that are far more significant (Reys, 2016, p. 2).

For an instance, the famous example is the cascading blackout that happened in the North America August 14, 2003, and deprived 50 million people of electricity supply. This had resulted in at least 11 deaths and caused serious damages that cost an estimated $6 billion (Minkel, 2008). This example, however, was the combination of human error and equipment failures, but it can perfectly demonstrate the possible scale of the causes of such errors.

Nicolas Reys, who is the Associate Director of the Control Risks' global cyber threat intelligence practice, in his article dedicated to Cyber Security Services, gives an example of inaccurate data readings transmitted for a certain period of time. According to him, this initial minor computing error can lead to wrong estimates indicating that it is required to increase the amount of supplied electricity for the considering premises. This would necessitate rerouting some of the existing energy supply to this facility, which, in turn, could culminate in increased costs for the affected business, as well as for the city, and a reduced pool of electricity for other companies and citizens.

Apart from that, taking existing cities into consideration, it is anticipated that they are going to experience the previously mentioned "shock therapy" (or "smart shock") (Sadowski & Pasquale, 2015), where the latest advanced technology is going to be integrated into an existing city architecture. However, it is immensely complicated to replace each part of the city's existing technology at once and substitute it with the latest technical innovations. Apart from that, the high-tech sphere is being continuously improved and developed and the idea of constant substitution of the current systems with the enhanced ones appears to be difficult to achieve.

This will facilitate another possible vulnerability, due to the fact that the certain part of legacy systems will remain to be used. A great number of smart technologies are involved in much older city infrastructure operating on software and technology created 20 or 30 years ago, which has not been constantly upgraded for some time, that also cannot be updated to the level of new implementations (Kitchin & Dodge, 2017, p. 5). The collaboration of modern and outdated technologies can result in poor maintenance. According to Robert Townsend, the legacy technologies can create inevitable vulnerabilities to newer systems by providing 'forever-day exploits' that can be interpreted as holes in legacy software products that vendors are not able to support anymore and therefore will never be patched (Kitchin & Dodge, 2017, p. 6). This means that errors may occur due to the different level of the systems upgrade.

The idea of the smart technology implementation conceals the real factors of possible problems caused by machine-to-machine interaction. Due to the above-mentioned reasons, it can be inferred that these possible issues are remaining without a constructive solution. It will require an extended period of time and a huge amount of financial investments in order to minimise the risk and to guarantee the proper system maintenance, while the Smart Cities projects have started to be widely implemented.

6.2 Cyber threats

6.2.1 Definition

In the world where people manage to execute numerous actions digitally, it is mandatory to ensure the users with the cybersecurity, which can frequently be equated to the personal safety. The *cybersecurity* can be defined as the variety of technologies, actions and system management the main aim of which is to provide the network and data protection from the potential cyberattacks (IT Governance, n.d.).

The term 'cyber threats' has become increasingly common in recent times. According to the CIO Whitepaper review (n.d.), a cyber threat can be defined as: "a malignant and

destructive act that tries to access a computer network through a data communications pathway, without gaining the right authorization or consent from the owners". It has also mentioned that these types of disruptive actions are frequently executed by hackers, who aim to gain an unauthorized access and steal a personal data of individuals in order to receive a financial gain or to perform troublesome and mischievous acts.

Cyber threats have a potential to lead to various collapses. Let alone the fact that they are capable of spoiling the reputation of a company or an individual by revealing personal information, or stealing the product designs and patents. The extent of the inflicted damage can become much higher. By getting an access to the confidential data belonging to different authorities, hackers can perform such criminal actions as manipulating governmental outcomes and proceedings, controlling power grids, misusing industrial control systems, stealing means from payment systems, etc. (CIO Whitepaper review, n.d.).

Such terms as cyberattack, cyber threat, and cyber risk complement each other. While the cyberattack is an illegal action that is executed by criminals, the cyber threat is the possibility that this action may happen, and the cyber risk is the approximate estimate of potential losses that may be incurred. There different ways in which the cyberattack can be performed depending also on the initial aim of a hacker (e.g. data collection, disruption of the system, etc.) (CyberSecurity Forum, n.d.).

Within the network of interconnected devices, the following types of cyberattacks should be considered: Distributed Denial of Service (DDoS) and Man-in-the-Middle (MITM).

- Distributed Denial of Service (DDoS)

The DDoS attacks can be defined as the subclass of the denial of service (DoS) attacks that are aimed to destroy online service by overwhelming it with fake traffic from the great number of collected devices (botnets). The DDoS assaults attempt to make a website and servers unavailable to its intended users (Imperva Incapsula, n.d.). The target devices include computers and other types of networked resources, for an instance, the IoT technologies (Cloudflare, n.d.).

These types of cyberattack can frequently last for the prolonged period and can severely disrupt any type of online network (e.g. decrease of revenue of the attacked organisation, reputation damage, etc.) (Imperva Incapsula, n.d.). For example, the attacker can prevent an internet user from accessing his email or other online accounts (online banking, etc).

Presumably, namely, the implementation of numerous unsecured IoT devices is enlarging the number of DDoS attacks. Alison DeNisco Rayome, in her article for the TechRepublic page, mentions the recent Reaper IoT-botnet that has hijacked the following IoT entities such as the internet-connected web cameras, security cameras, and digital video

recorders. The extent of the attack is growing, due to the fact that infected devices share malware to other vulnerable devices within the particular network. According to Ashley Stephenson, the CEO of Corero, the IoT botnets have a potential to lead to Internet chaos (Rayome, 2017).

- Man-in-the-Middle (MITM)

Man-in-the-Middle is the type of the cyberattack that is executed by intercepting the communication between the user and the actual server by the third party (attacker), in order to gain control over the user's information (Simko, 2016). In the majority of cases, the user is not able to detect the attack as the infected device proceeds with the proper function, as if it is connected to the actual server. However, the attacker obtains all data that is transmitted on both sides of the parties and is able to manipulate the gathered information (e.g. change money transaction) (Bizety, 2016).

Due to the fact that various IoT products contain the vast number of security vulnerabilities, the risk of the possible attack is increasing. As Smart Cities is the concept implementing the endless variety of automated and interconnected tools, it causes a further serious concern that lies in the increase in security vulnerabilities caused by the possible disruption and hacking of smart technologies. The structure that is composed of multiple connected networks is extremely vulnerable to the exposure of self-propagating malware (Reys, 2016, p. 2). Apart from that, as it has been already mentioned in the previous chapters that the smart systems will be based on the gathering and storing of such data as the healthcare information, geographical tracking, social security numbers, etc. This data is considered to be easily commoditised and acquiring an easy access to it can lead to the leakage of serious data (Reys, 2016, p. 2).

It can be inferred that the technology that is implemented with the initial purpose of making cities smarter, by the increase in connectivity and automation thereby making them more hackable. Therefore, the next subchapters will focus on cybersecurity-related problems and the main reasons for their possible occurrence.

6.2.2 Cybersecurity problems

Foremost, it is important to consider the types of risks that can be entailed by cyberattacks. Two main security risks will be faced: an extent to which 'intelligent technologies' are vulnerable to being hacked and the security of stored, operated and shared data across the network. The second risk complements the first one due to the improper access to stored information which is frequently caused by the security weaknesses of the system's

components, architecture and operation (Kitchin & Dodge, 2017, p. 4). This subchapter will be concentrating on the vulnerabilities of city infrastructures rather than on data security.

- Cascading errors

Modern society is not generally able to realise the possible cost of damage inflicted by the hacked critical infrastructures. Even the small-scales cyberattacks have the potential to cause the above-mentioned cascade effect that is not necessarily induced by the error in machine-to-machine interaction. The consequences of cyberattacks that occurred inside the network of the highly interconnected entities can be rapidly transmitted among these devices (Kitchin & Dodge, 2017, p. 6). For an instance, in case of a cyberattack launched on an electrical power infrastructure, the disruptive effects can cascade into the city operation centre from which it can further cascade to the other related systems (e.g. traffic management, emergency services…). This is one of the major risks that can be incurred by the linked systems, in contrast to approaches that are engaging the Information silo, which include the operation of data separated from other information management systems (Investopedia, n.d.; Kitchin & Dodge, 2017, p.8).

In addition, in case of hackers succeeding in damaging the electricity grid that is performing an important task of powering multiplicity of infrastructures, the enormous cascade effects can be exerted. The history has already demonstrated numerous examples illustrating the extents of such cyberattacks. For an instance, in December 2015, a group of hackers successfully executed a cyberattack on Ukrainian electric utilities that lead to the power shutdown to hundreds of thousands of consumers (Science Friday, 2018).

- Hacking Smart Meters

The concerns dealing with the insecurity of electricity supply are not necessarily globally extended; however, they can contain a local character, as a separate individual whose household is equipped with the Smart Meter can be subjected to the cyberattacks as well. The analogue meters are gradually replaced by the modern smart meters, which are intended to enhance efficiency by an automatic capture of information relating to the consumer's electricity consumption and transmitting it to the companies managing electricity supply (Sunshine, 2018).

Although the smart electricity meters are rapidly increasing in its usage, including the approximate number of 100 million of devices installed around the world, the security experts seriously doubt their security (The Guardian, n.d.). There is an arising number of warnings about the feasible viruses transmitted through the different devices can cause the disconnection of individual energy supplies. In addition, these utilities could even be hacked and used for terrorism (Meadows, 2017).

According to the Netanel Rubin, who is the co-founder of the security firm Vaultra, has predicted the rise in attempts to hack smart utilities. Due to the lack of security in the implemented smart devices, the hacker is potentially able to get excess to the gathered information about the amount of used electricity. The criminals can execute the false billing operations by sending the requests for paying the fake invoices to the smart meter owners. The hacker can gain the power over the consumer's electricity consumption, over the smart utilities that are connected the electricity and over the meter's software (The Guardian, n.d.).

The cases complementing the security worries have already happened. The famous example occurred in 2009 when FBI investigated the power thefts executed through the smart meters in Puerto Rico. As cited in the KrebsonSecurity (2018): "The FBI said it believes former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash and training others to do so". This massive fraud enabled hackers to steal hundreds of millions of dollars through the smart meters.

- Hacking traffic systems

The major issue of security is spreading over each sphere of city managing that is implying the use of automated technology. Nowadays, the wireless communication is frequently implemented within the traffic systems, due to the fact that it helps to achieve the coordination of these systems despite the geographic distribution of roadways. Apart from that, the cost of wireless connection between the intersections is considerably lower than the physical one (Ghena et al., 2014, p. 1). However, the remote access to these systems raises the possibility of cyberattacks.

For an instance, in case of the hacker gaining control over the wireless traffic signal system, this can potentially enable him to create huge traffic jams or cause massive accidents. Apart from that, the attack may lead to the serious disruption of the network completely disabling the city municipals to manage the situation.

Expressing concerns about this problem, the group of computer science researchers working with professor J. Alex Halderman, in 2014, made an experiment that was held in order to test the security of traffic infrastructure of Michigan. The main task was to simulate the cyberattack and analyse the extent of system security. Due to the existing errors in the system design, the researchers were able to access the traffic lights system that allowed them to control the light signals and change them on command. These obtained results demonstrate that the real attacker would be able to control the traffic infrastructure to cause disruption leading to the citizens' safety violation (Computer Science and Engineering, University of Michigan, 2014).

The cyberattacks are not considered to be the recent novelty. Nevertheless, the scale of Smart technologies realisation is gradually extending. From the above-mentioned examples, it can be concluded that these innovations are not different by containing the variety of risks that are dealing with security. Hackers are followed by different motivations that might remain timeless (e.g., theft, impersonation, vandalism, malicious attack). However, the way of performing the cyberattacks has changed. As cited in Kitchin and Dodge, (2017, p.3): "Because smart city technologies rely on networked digital computation, exploits of their vulnerabilities can be undertaken at distance and attacks can be masked, reducing the risk of detection and capture for perpetrators". This has the potential to negatively affect the great number of different cities, as the attackers would be able to simultaneously conduct virtual criminality and gain unauthorised access to multiple networks.

6.2.3 Reasons for Cybersecurity issues

Evidently, the security problems are going to significantly influence each sphere of city infrastructure. The security vulnerabilities of smart technologies are caused by numerous factors the majority of which are dealing with the facilities governing the cities. It is essential to list and describe the most common reasons for the cybersecurity issues.

- Lack of Security Testing

Unfortunately, the security does not appear to be the main priority in the projects based on the supply of connectivity of devices through the Internet of Things that are widely distributed among the city developers. Moreover, the IoT concept is highly controversial and contains the poor security practices on industrial systems (Cerrudo, 2015, p.7).

The implementation of connected appliances does not frequently involve the test of the extent to which the device is vulnerable to be hacked. In contrast to the marketing materials where the smart technologies are presented as the network of secure data transmission, many vendors experience the negligible amount of security features inserted into their smart products (Kitchin & Dodge, 2017, p. 7). Apart from that, a considerable number of cities does not control the security level of the acquired devices (Kitchin & Dodge, 2017, p. 8).

For an instance, Cesar Cerrudo in his research paper "An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks" has mentioned such important cities as Washington DC, New York, San Francisco, London, Lyon, and Melbourne which contain the approximate number of 200,000 assailable sensors that are embedded in the traffic control systems (Cerrudo, 2015, p. 8). He has also referred to other researchers by inferring that the critical infrastructures are supplemented with appliances lacking the security testing.

- Encryption and Issues

The communication channels between connected devices have to be protected. Due to the fact that IoT technologies are transmitting signals wirelessly, this simplifies the task of the attacker to manipulate these signals. For this reason, in order to estimate whether the device can trust the particular remote system, encryption and authentication technologies are used. However, there is an existing problem with the proper encryption implementation within the smart devices.

According to Cerrudo (2015), these problems are caused by outdated and weak encryption algorithms and by poor encryption key management. The majority of issues is relating to the weak key generation, fixed keys, shared keys, etc. Apart from that, occasionally, the system contains the certain encryption options that are capable to secure its operation; however, the cities do not merely activate these options. This may happen due to the lack of security knowledge or the complexity of the realisation (Cerrudo, 2015, p.8).

This results in the poor security of communication that enables the hacker to intercept the communication and to perform different manipulations the devices within the attacked network (Cerrudo, 2015, p. 9).

- Complexity of the system

Another essential vulnerability is the immense complexity of the Smart City network. The wide diversity, huge number of interdependences and large attack surfaces complicate the estimation of the possible risks related to the end-to-end security (Kitchin & Dodge, 2017, p.6). Even if the independent systems will reach the proper level of security, connecting them with other systems can introduce the new risk with the decrease of security level.

Apart from that, it is harder to provide the ongoing maintenance and regular update of the entities when the network comprises numerous interdependences (Kitchin & Dodge, 2017, p.6).

By summarizing the Chapter 5, it can be inferred that, due to the above-mentioned reasons, the smart technologies are enlarging the surface for the cyberattacks and create further security vulnerabilities. At present, this issue is largely ignored by municipal services. In order to prevent the further extension of the mentioned vulnerabilities, it is crucially important to develop new strategies that will eliminate or highly reduce the possibility of their occurrence. The security tests have to be done in order to guarantee the secure work of appliances before their implementation into the city's infrastructure.

7. Conclusion

The concept of the Smart Cities is rapidly evolved by the collaboration of intelligent developers all around the world. The smart technologies are widely implemented in different spheres of urbanistic life. However, the positive perception of the term can seriously distort the picture. Each human invention contains disadvantages that are supposed to be studied in order to avoid their misuse. The aim of my thesis was to present and examine the negative impacts that can be exerted and influence the life of the citizens living in the highly technological environment.

After analysing the definition of the Smart City, and determining the main entities that are frequently associated with its realisation, I have considered two major issues which are the serious lack of the citizens' security caused by the constant data collection and vulnerabilities that may occur due to mistakes during machine-to-machine interactions and poor cybersecurity of the network devices.

From the information revealed in this thesis, it can be inferred that there is a huge number of existing issues that are dealing with data collection, storage, and quantification that are merely ignored by the city governance. This may result in threating and manipulation of society and governmental invasion of personal privacy. Surveillance is justified on the grounds that safety is more important than privacy. Such techniques as constant monitoring and predictive policing are the examples that perfectly illustrate this.

Referring to the chapter dedicated to the vulnerabilities of the systems that appear due to the concept's implementation and are frequently hidden or, merely, are not mentioned in the marketing materials of smart technologies, it can be concluded that the two main problems arise. Firstly, mistakes caused due to M2M communication, where the humans' control over the process is reduced to the minimum, raise the possibility of cascading errors and errors that may occur due to the different upgrade level of the network devices. Secondly, the poor security and encryption in such complex systems may result in the execution of cyberattacks that can seriously damage the city's maintenance.

In conclusion, it is essential to affirm that the truly Smart City accepts flexible and spontaneous changes and is influenced not only by the city municipals, however, is also adjusted by the initiatives of its 'smart' citizens. These initiatives will be designed to neutralise the above-mentioned negative impacts and will simultaneously contribute to the technological development. I sincerely believe that it is possible to implement modern technology without causing serious harm to security and safety of the citizens.

List of references

Aktiengesellschaft. (2012). In The Free Dictionary by Farlex. Retrieved from: http://financial-dictionary.thefreedictionary.com/Aktiengesellschaft

Amsterdam Smart City: https://amsterdamsmartcity.com/projects

Ball, J. (2013, June). NSA data surveillance: how much is too much? In The Guardian. Retrieved from: https://www.theguardian.com/world/2013/jun/10/nsa-metadata-surveillance -analysis

Barrett, D. (2013, July). One surveillance camera for every 11 people in Britain, says CCTV survey. Retrieved from: https://www.telegraph.co.uk/technology/10172298/One-surveillance -camera-for-every-11-people-in-Britain-says-CCTV-survey.html

Bernstein, P. (2015, August 19). Using ICT to Make Smart Cities Smart. Next Generation Communications. Retrieved from: http://next-generation-communications.tmcnet.com/topics/industries/articles/408542-using-ict-make-smart-cities-smart.html

Brakel, R., & Hert, P. (2011-3). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. Retrieved from: http://www.vub.ac.be/LSTS/pub/Dehert/378.pdf

Bulkeley, H., et al. (2017). Urban living labs: governing urban sustainability transitions. Science direct. Retrieved from: https://ac.els-cdn.com/S1877343517300325/1-s2.0-S1877343517300325-main.pdf?_tid=5b667888-d9d9-11e7-b76d-00000aab0f01&acdnat=1512491502_945bf98f3b5da7b508ef71195c4b7f61

Campbell-Dollaghan, K. (2014, April). Police Are Testing a "Live Google Earth" To Watch Crime As It Happens. Retrieved from: https://gizmodo.com/police-are-testing-a-live-google-earth-to-watch-crime-1563010340

Centro de Operações Prefeitura do Rio de Janeiro. (2017, August). Veja Rio. Retrieved from: https://vejario.abril.com.br/cidades/centro-de-operacoes-rio-tem-o-quarto-chefe-em-oito-meses/

Cerrudo, C., (2015). An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks. Retrieved from: https://ioactive.com/wp-content/uploads/2018/05/IOActive_HackingCitiesPaper_cyber-security_CesarCerrudo-1.pdf

City. (n.d.). In Meriam-Webster Dictionary. Retrieved from: https://www.merriam-webster.com/dictionary/city

Cohen, B. (2013, November 14). The 10 Smartest Cities In North America. Retrieved from: https://www.fastcompany.com/3021592/the-10-smartest-cities-in-north-america

Cyber Attacks: Classifications & Taxonomies. (n.d.). In CyberSecurity Forum. Retrieved from: http://cybersecurityforum.com/cyber-attacks/

Degtereva, E. (2017, September 26). Smart City: cities of the future that already exist [In Russian]. Retrieved from: https://mir24.tv/news/16269345/smart-city-goroda-budushchego-kotorye-uzhe-sushchestvuyut

Distributed Denial Of Service Attacks. (n.d.). DDOS Protection Center: Imperva Incapsula. Retrieved from: https://www.incapsula.com/ddos/denial-of-service.html

Doctorow, C. (2014, June). Riot control drone that fires paintballs, pepper-spray and rubber bullets at protesters. Retrieved from: https://boingboing.net/2014/06/17/riot-control-drone-that-paintb.html

Edward Snowden Biography. (2018, February). A&E Television Networks. Retrieved from: https://www.biography.com/people/edward-snowden-21262897

E-estonia: https://e-estonia.com/

Elfrink, W. (2010). Smart Connected Life: The Cisco pavilion guide. Retrieved from: https://www.cisco.com/c/dam/global/zh_cn/assets/expo/pdf/smart_connected_life_guide_en.pdf

Evans, D. (2011, April). The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Cisco Internet Business Solutions Group (IBSG). Retrieved from: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

FBI: Smart Meter Hacks Likely to Spread. (2018, May). In KrebsonSecurity. Retrieved from: https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

Finch, K., & Tene, O. (2016, March). Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town. In Fordham Urban Law Journal. Retrieved from: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2549&context=ulj

Florida, R. (2011, September 15). Why cities matter. Retrieved from: https://www.citylab.com/design/2011/09/why-cities-matter/123/

Ghena, B., et al. (2014, August). Green Lights Forever: Analyzing the Security of Traffic Infrastructure. Retrieved from: http://www.eecs.umich.edu/eecs/about/articles/2014/traffic-woot14.pdf

Greenfield, A. (2012, December). Another city is possible: The "smart city" from above and below. Retrieved from: https://files.lsecities.net/files/2013/01/06_03_Greenfield1.pdf

Hester, J.L. (2017, April). How to Disappear. Retrieved from: https://www.citylab.com/life/2017/04/how-to-disappear/524007/

Höflehner, T., & Zimmermann, F.M. (2016, April). An Innovation in Urban Governance: Implementing Living Labs and City Labs through Transnational Knowledge and Experience Exchange. Regional Studies Association Annual Conference. Retrieved from: http://www.regionalstudies.org/uploads/Hoeflehner_Zimmermann_An_Innovation_in_Urban_Governance.pdf

Hoskinson, C. (2014, November 20). NSA chief: China, other countries can hack into U.S. electric grid. Washington Examiner. Retrieved from: http://www.washingtonexaminer.com/nsa-chief-china-other-countries-can-hack-into-u.s.-electric-grid/article/2556442

How Do You Prevent Russia From Hacking Into The U.S. Power Grid? (2018, March). In Science Friday. Retrieved from: https://www.sciencefriday.com/segments/how-to-prevent-russia-from-hacking-into-the-u-s-power-grid/

How Many CCTV Cameras in London? (n.d.). Caught on Camera. Retrieved from: https://www.caughtoncamera.net/news/how-many-cctv-cameras-in-london/

Information Silo. (n.d.). In Investopedia. Retrieved from: https://www.investopedia.com/terms/i/information-silo.asp

Keeton, R. (2015, April-June). When Smart Cities are Stupid. Retrieved from: http://www.newtowninstitute.org/spip.php?article1078

Kitchin, R. (2014, February). The real-time city? Big data and smart urbanism. In GeoJournal. Retrieved from: https://link.springer.com/article/10.1007%2Fs10708-013-9516-8

Kitchin, R., & Dodge, M. (2017, February). The (in)security of smart cities: vulnerabilities, risks, mitigation and prevention. Retrieved from: https://osf.io/preprints/socarxiv/f6z63

Knobbe, M., & Schindler, J. (2017, September). Interview with Edward Snowden: 'There Is Still Hope - Even for Me'. Retrieved from: http://www.spiegel.de/international/europe/edward-snowden-interview-there-is-still-hope-a-1166752.html

Kuurme, K. (2016, March 13). A peek into our digital future: Estonia's e-Residency program. TEDxMidAtlantic. Retrieved from: https://www.youtube.com/watch?v=QY_BArNLASY

Laartz, J., & Lülf S. (2014). PARTNERING TO BUILD SMART CITIES. Retrieved from: http://webcache.googleusercontent.com/search?q=cache:U4BGCzUhgNsJ:www.mckinsey.com/~/media/mckinsey/dotcom/client_service/Public%2520Sector/GDNT/GDNT_SmartCities_v5.ashx+&cd=1&hl=ru&ct=clnk&gl=cz

Lerman, T. (2018, February). 5 Data Center Real Estate Trends To Watch For. Retrieved from: https://www.bisnow.com/atlanta/news/data-center/5-data-center-real-estate-trends-to-watch-out-for-84281

Lufkin, B. (2017, October). Could Estonia be the first digital country? Retrieved from: http://www.bbc.com/future/story/20171019-could-estonia-be-the-first-digital-country

MAKiPI (2015, September). "Smart cities" and total control [In Russian]. Retrieved from: https://makipi.livejournal.com/11244.html

Mattern, F., & Floerkemeier, C. (n.d.). From the Internet of Computers to the Internet of Things. Retrieved from: http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf

Meadows, S. (2017, August). Six reasons to say no to a smart meter. Retrieved from: https://www.telegraph.co.uk/money/consumer-affairs/six-reasons-say-no-smart-meter/

Mesmer, P. (2017, May). Songdo, ghetto for the affluent. Retrieved from: http://www.lemonde.fr/smart-cities/article/2017/05/29/songdo-ghetto-for-the-affluent_5135650_4811534.html

Mesmer, P. (2017, May). Songdo, ghetto for the affluent. Retrieved from: http://www.lemonde.fr/smart-cities/article/2017/05/29/songdo-ghetto-for-the-affluent_5135650_4811534.html

mGovernment: Mobile/Wireless Applications in Government. (n.d.). Retrieved from: http://www.egov4dev.org/mgovernment/

Minkel, J.R. (2008, August). The 2003 Northeast Blackout - Five Years Later. Retrieved from: https://www.scientificamerican.com/article/2003-blackout-five-years-later/

Mitchell, S., et al. (2013). The Internet of Everything for Cities: Connecting People, Process, Data, and Things To Improve the 'Livability' of Cities and Communities. Cisco and/or its affiliates. Retrieved from: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/everything-for-cities.pdf

Morsella, C. (2009). Cisco Spokesperson Says "Smart Grid May Be 1,000 Times Larger than the Internet". Retrieved from: http://greeneconomypost.com/smart-grid-communications-networking-3319.htm

Neidhart, C. (2018). Welcome To Songdo, South Korea: The Smartest Of Smart Cities. Retrieved from: https://www.worldcrunch.com/smarter-cities-1/welcome-to-songdo-south-korea-the-smartest-of-smart-cities

Nesbitt, P. (2012). IBM Intelligent Operations Center for Smarter Cities. Retrieved from: http://www.redbooks.ibm.com/abstracts/tips0930.html?Open

Nesti, G. (2017, September). Co-production for innovation: the urban living lab experience. Retrieved from: http://www.tandfonline.com/doi/full/10.1080/14494035.2017.1374692

Newitz, A. (2014). The Dark Side of the "Smart City". Retrieved from: https://io9.gizmodo.com/the-dark-side-of-the-smart-city-1512608758

Nordrum, A. (2016, August 18). Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. Retrieved from: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

O'connell, P. L. (2005, October). Korea's High-Tech Utopia, Where Everything Is Observed. In The New York Times. Retrieved from: http://www.nytimes.com/2005/10/05/technology/techspecial/koreas-hightech-utopia-where-everything-is-observed.html

Okorie, G. (2015, July). Urbanization Problems In Developing Countries. Retrieved from: https://www.linkedin.com/pulse/urbanization-problems-developing-countries-golfer-okorie

Palmisano, S.J. (2010, June 2). Building a smarter planet, city by city. Retrieved from: https://www.ibm.com/smarterplanet/us/en/smarter_cities/article/shanghai_keynote.html

Palvia, & Sharma. (n.d.). E-Government and E-Governance: Definitions/Domain Framework and Status around the World. Retrieved from: http://csi-sigegov.orgwww.csi-sigegov.org/1/1_369.pdf

Perera, C., Liu, C.H., & Jayawardena, S. (2015, December 9). The Emerging Internet of Things Marketplace: From an Industrial Perspective: A Survey. Retrieved from: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7004800

Predictive policing: Don't even think about it. (2013, July). In The Economist. Retrieved from: https://www.economist.com/news/briefing/21582042-it-getting-easier-foresee-wrongdoing-and-spot-likely-wrongdoers-dont-even-think-about-it

PredPol: http://www.predpol.com/

Protecting IoT Against Man-in-the-Middle Attacks. (2016, February). In Bizety. Retrieved from: https://www.bizety.com/2016/02/12/protecting-iot-against-man-in-the-middle-attacks/

Rayome, A. D. (2017, November). DDoS attacks increased 91% in 2017 thanks to IoT. Retrieved from: https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/

Researchers Demo Hack to Seize Control of Municipal Traffic Signal Systems. (2014, August). In Computer Science and Engineering, University of Michigan. Retrieved from: http://www.eecs.umich.edu/eecs/about/articles/2014/Green-Lights-Forever.html

Reys, N. (2016). SMART CITIES AND CYBER THREATS. Retrieved from: https://cdn-prd-com.azureedge.net/-/media/corporate/files/our-thinking/insights/smart-cities-and-cyber-threats/smart-cities-article.pdf?modified=20170710141720

Rise of the machines: who is the 'internet of things' good for? (2017). In The Guardian. Retrieved from: https://www.theguardian.com/technology/2017/jun/06/internet-of-things-smart-home-smart-city

Robles, A.G., et al. (2015). Introducing ENoLL and its Living Lab community. European network of Living Labs. Retrieved from: https://issuu.com/enoll/docs/enoll-print

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March). How Trump Consultants Exploited the Facebook Data of Millions. In The New York Times. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Rouse, M. (2016, July). Internet of things. IoT Agenda. Retrieved from: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Rouse, M. (2017, October). Smart home. IoT Agenda. Retrieved from: http://internetofthingsagenda.techtarget.com/definition/smart-home-or-building

Sadowski, J., & Pasquale, F. (2015, July). The spectrum of control: A social theory of smart city. Retrieved from: http://firstmonday.org/article/view/5903/4660

Simko, C. (2016, February). Man-in-the-Middle Attacks in the IoT. Retrieved from: https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot/

Smart City is built in South Korea. (n.d.). In Econet. [In Russian]. Retrieved from: https://econet.ru/articles/125848-v-yuzhnoy-koree-stroyat-umnyy-gorod

Smart electricity meters can be dangerously insecure, warns expert. (n.d.). In The Guardian. Retrieved from: https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers

Smart. (n.d.). In Meriam-Webster Dictionary. Retrieved from: https://www.merriam-webster.com/dictionary/smart

Street-level surveillance. (n.d.). In Electronic frontier foundation. Retrieved from: https://www.eff.org/ru/pages/automated-license-plate-readers-alpr

Sunshine, W. L. (2018, April). Pros and Cons of Smart Electric Meters. Retrieved from: https://www.thebalancesmb.com/pros-and-cons-of-smart-meters-1182648

Sunshine, W.L. (2017, October 12). Pros and cons of Smart Electric Meters. Retrieved from: https://www.thebalance.com/pros-and-cons-of-smart-meters-1182648

Svetlik, J. (2015, July 22). Rise of the smart city: The awesome and scary reality of future urban living. Retrieved from: https://www.wareable.com/index.php/internet-of-things/the-awesome-and-scary-future-of-our-cities-2025

The Advantages and Disadvantages of Implementing Police Body Cameras and a Look at the Surrounding Current Legislative Activity. (2015, March 17). Retrieved from: https://www.slideshare.net/NoellMartinez/research-paper-advantages-and-disadvantages-of-police-body-cameras

The Generator Project. (n.d.). In Interactive Architecture Lab. Retrieved from: http://www.interactivearchitecture.org/the-generator-project.html

The good, the bad and the inevitable: The pros and cons of e-government. (2008, February 14). The Economist. Retrieved from: http://www.economist.com/node/10638105

The Internet of Things. (n.d.) Suny Cortland. Retrieved from: https://sites.google.com/a/cortland.edu/the-internet-of-things/disadvantages

The President's National Security Telecommunications Advisory Committee. (2014, November 19). NSTAC Report to the President on the Internet of Things. Retrieved from: https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf

The Smart City. (2016, March). In Kista Science City. Retrieved from: http://international.stockholm.se/city-development/the-smart-city/

Townsend, A.M. (2014). Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia. W.W. Norton & Company.

United Nations: E-government Survey 2014: E-government for the future we want. (2014). Department of Economic and Social Affairs. Retrieved from: https://publicadministration.un. org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf

Verma, P.K., et al. (2016, March). Machine-to-Machine (M2M) communications: A survey. In Journal of Network and Computer Applications. Retrieved from: https://www.sciencedirect.com/science/article/pii/S1084804516000990

What are Living Labs: Common elements in Living Labs. (n.d.). ENoLL. Retrieved from: http://www.openlivinglabs.eu/node/1429

What is a Smart Meter? (n.d.). Smart Energy GB. Retrieved from: https://www.smartenergygb.org/en/about-smart-meters/what-is-a-smart-meter

What is Cyber Security? (n.d.). In IT Governance. Retrieved from: https://www.itgovernance.co.uk/what-is-cybersecurity

What is cyber threats? (n.d.). In CIO Whitepaper review. Retrieved from: https://whatis.ciowhitepapersreview.com/definition/cyber-threats/

What is the DDoS attack? (n.d.). In Cloudflare. Retrieved from: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

What is the Smart Grid? (n.d.). U.S. Department of Energy: Office of Electricity Delivery & Energy Reliability. Retrieved from: https://www.smartgrid.gov/the_smart_grid/smart_grid.html

Wichmann, B. (2014, December 17). THE PROS AND CONS OF SMART GRID TECHNOLOGY. Retrieved from: http://artemia.com/the-pros-and-cons-of-smart-grid-technology/

Winkel, E. (2011, October). Camera surveillance in Amsterdam, does it work? Retrieved from: http://www.eukn.eu/e-library/project/bericht/eventDetail/camera-surveillance-in-amsterdam-does-it-work/

Zoonen, L. (2016). Privacy concerns in Smart Cities. Retrieved from: https://ac.els-cdn.com/S0740624X16300818/1-s2.0-S0740624X16300818-main.pdf?_tid=f7cb9920-e622-4922-ad04-18174c9737a8&acdnat=1520685066_9460ee2b1dfcc35962f6aae793ab3a2c

List of abbreviations

AG – from the German *Aktiengesellschaft*, publicity-traded company

ALPR – Automatic number-plate recognition

CCTR – Central Camera Surveillance Room

CCTV – Closed-circuit television camera

CEO – Chief Executive Officer

CEO – Chief Executive Officer

DDoS – Distributed Denial-of-Service

DNA – Deoxyribonucleic acid

DoS – Disk Operating System

IBM – International Business Machines

ID – Identity Document

IoE – Internet of Everything

IoT – Internet of Things

M2M – Machine to machine

MITM – Man-in-the-Middle

NSA – National Security Agency

PredPol – Predictive Policing

SC – Smart City

SG – Smart Grid

SH – Smart Home

SW – Smart wearable

TED – Technology Entertainment Design

ULL – Urban Living Labs

List of figures

List of tables