Attacks against data security in smart cities: hypothetical scenarios or reality?

Irina-Ana DROBOT,
Technical University of Civil Engineering Bucharest, Faculty of Engineering in Foreign Languages, Department of Foreign Languages and Communication, Bucharest, Romania
anadrobot@yahoo.com

Abstract
The Objective is to show how changes in our lifestyle, which becomes more comfortable due to technological advancement, can lead to changes in which attacks, theft and various frauds can occur in smart cities. We need to be aware of risks. Prior work includes selected case studies and hypothetical risks scenarios, studied focusing not on the information, but on the way we relate to it. The 2018 Atlanta ransomware attack of the computer system of an entire smart city led to shutting down the municipal course, and to not allowing the citizens to pay their water bills and tickets for city traffic. In 2014, there was an attack on smart household appliances, worldwide, and home-networking routers were damaged. In Los Angeles, in 2016, an incident delayed work at MedStar hospital chain. The cyberattack caused data breaches in the healthcare industry, since medical equipment, such as pacemaker devices and MRI machines rely on information which expose them to risks. Hypothetical scenarios include cyberattacks damaging the way traffic functions. Approach: Data Security will be analysed from a psychological and cultural perspective, related to the anthropology of urban communities, and to the way in which individuals understand their right to personal space, data privacy, and the protective role of the cities. Case studies in previous research and news will be analysed. Results: Regarding the large-scale damage once cyberattacks occur, at the level of various areas of activity, affecting the entire city, what measures are taken by the European Union? Is digital democracy a simple utopia? Implications: Knowledge of previous experience means prevention for authorities and precaution for citizens. Value: Human beings need to cooperate with technology, but not passively. They need to be aware of its limits and not consider it a magical solution. Technology has shaped our urban culture and mindset.

Keywords: culture, values, mindset, practices.

1. Introduction
We can regard smart cities in the context of the phenomenon of the fast rate of urbanization [1]. Urbanization has been ongoing since the industrialization age, which was the first time when technological development reached a very high level, during the Victorian age. It continued further on, until today, until we reached the level of smart cities. Urbanization has meant a constant move of the population from rural to urban areas, to the point where the majority of the population will be living in cities. Since cities are the most frequent form of living and organization in today's world, and since urbanization is on the increase, we need to address the topic and to raise awareness regarding issues we are commonly confronting with today all over the world. We are, nowadays, organized in international, supranational and global communities, meaning that, next to our national specificities and forms of organizations, we can find urban culture which is present worldwide.

Cities are associated, especially, with "a better living environment" [1]. This means services and security. The comfort ensured by cities is related to the following services provided by cities: "water supplies and sewerage systems, residential and office buildings, education and health services and convenient transportation" ([2], mentioned in [1]). Cities, ever since ancient times, also meant protection for citizens, next to all the confort of daily living. We can be surprised at the high level of development of these services ever

since ancient times, yet the development is ongoing and adapting to the new possibilities of the cities, reaching the latest level of development, the smart city.

The smart city appeared as an answer to accommodate the needs of a continuously growing population [3], together with the organization and comfort it needs in case of a large population in the urban areas. These aspects lead to reliance on technology by local governments for ensuring the management of the city [3]. The management of the city in a smart city means using technology "to support a higher quality of urban spaces and a better offering of public services" [3].

Smart cities rely on technology, yet there are drawbacks to technology as much as there are advantages. One of the main issues can be, just as in the case of using computers and smartphones, and in the case of their software and applications, the security, theft and malfunctioning of data. It appears that thieves have adapted to the virtual environment, and to the possibilities offered by technology. Technology, through the use of various applications, has changed the way we relate to everyday life in the city, from using paid parking services to self-checkout, and to getting our public transport tickets, e.g. for bus and train, online, or using text messaging instead of relying on a seller. Even medical devices and smart household appliances, as well as traffic, can function in a smart city based on technology. Everything is programmed and the smallest problem with technology can ruin the functioning of a large segment of our lives in the city, if not the entire city.

We can notice how technology and culture, although at first sight unrelated, can be regarded as intertwined. Once we understand culture as an everyday life practice, we can see how technology has become one, in our daily lives. City life includes images of people of all ages with their smartphones, sending messages, checking social media, paying for various services, taking photographs and selfies. Contemporary art started to include selfies to the point where some art exhibitions, such as MoBU, recently organized as an art fair at ROMEXPO in Bucharest, Romania, during May 29-June 2, 2024, has considered telling visitors on a notice board to grab a doll and take a selfie. This is a form of interactive art, and selfies has also been included within various art pieces in the case of certain artists.

The way we use services in the smart city, which is a city relying on technology and which is developing all over the world continuously, can be considered part of our urban culture. We have come to perceive all this either as extremely comfortable, or as threatening and scary, once we do not know how to use it and once we have been confronted with various problems related to their use. For example, self pay in supermarkets has been, at least in some stores in Bucharest, Romania, quite recently a subject of debate in social media, as the self pay points were malfunctioning and did not help save time, but on the contrary, they made customers lose time. The problem was in a supermarket from the Auchan chain of stores, where all human cashiers were replaced by self checkout where customers had to scan their bought items themselves.

Still, these are just a few aspects of everyday life in a smart cities. We can also consider smart buildings, with plants and flowers on their surface, as well as with what look like gardens on top. Green spaces, and public parks are now the norm. We can consider how,

during the electoral campaign of 2024, before the elections in June in Bucharest, Romania, in district 6, Drumul Taberei neighbourhood there was an announcement about experimental green spaces with poppies where people were encouraged to take selfies.

Where do risks come in smart cities? Which data security issues can occur, even if, having in mind the comfort and utopia of everyday life in smart cities come in? Are citizens truly prepared for these data security attacks and why?

2. Materials and Methods

We can notice a contrast between the security of smart cities, which, through their use of high technology, can ensure "green environment and well-being for citizens" (R. P. Dameri, et al., 2013), social, "cultural needs" [4], entertainment, together with safety, promising a fantasy, utopic world, on the one hand and, on the other hand, the threat against the security of this very well-organized structure, revealing a distopic world, on the other hand. This contrast, however, regarding life in cities has existed since old times, when armed wars would threaten the stability of life in the city. We can speak of an adaptation to today's living conditions and technology when we consider attacks against data security.

Since a smart city includes optimization of "both tangible (e.g. transport infrastructures, energy distribution networks, and natural resources) and intangible assets (e.g. human capital, intellectual capital of companies and organizational capital in public administration bodies)" [5], the attacks against data security can target precisely these assets.

While life in a smart city can be associated, mostly, with entertainment and comfortable, peaceful, living conditions, once we look at cases that have occurred and at hypotheses regarding data security attacks, we notice how many risks are around and how many issues have actually occurred.

Examples of attacks against data security are presented in Fig. 1, taken over from a research paper [5]. As we can see, these attacks have targeted everyday life, housework appliances, such as smart refrigerators, tourists' hotels, and, thus, hotel businesses, in the case of a lock system, in most USA hotels, medical devices such as insulin pumps which would forget the right dosage after their batteries were changed and, therefore, could be dangerous to patients, the medical system, including surgery activity in hospitals, caused by devices that could be attacked since data was vulnerable due to its availability needed in order to purchase various devices, e.g. pacemakers and MRI machines, and, last but not least, passports, which could be copied using an RFID scanner, due to "unsecured wireless nodes" [5].

Fig. 1 below present each case, with its identifying details, in brief, including the year and place where they occurred, below the title line which helps identify the many situations that can become, from facilities and tools for a comfortable, highly-technologized life, sources of complete danger:

Fig. 1. Examples of Attacks on Data Security that have occurred in Smart Cities.
Source: Article shown in reference [5]

We can range the cases of attacks against data security, function of their consequences, according to the domains of activity and areas in life that they can affect, from mild to severe, while keeping in mind alternative solutions that may be found. If we look at the consequences related to the health and even life of patients in hospitals or people suffering from various conditions such as diabetes, we realize that technology has helped work in the medical field to become more and more efficient, and to help more patients in the course of a very short time by using high technology medical devices. The high technological development, through these high performance medical devices, can also help persons suffering from diabetes to have access to insulin pumps and be independent in their need for insulin through the very use of such devices. However, in Fig. 1 we notice that, once there is the slightest malfunctioning for various reasons, e.g. in the case of the battery exchange of insulin pumps, not only attacks against data security, then the lives of so many people dependent on and in need for treatment using these smart medical devices and needing them to be provided by the hospital will have their lives endangered. The health of the citizens is one important aspect of the security of any city. The malfunctioning of medical devices can be considered the most severe. Indeed, we notice how attacks against data security have led to an entire hospital chain to be "paralyzed" in its activity, failing to provide care, and how changing the batteries on insulin pumps caused them to reset and to no longer deliver the right dosage of insulin to the person suffering from diabetes, which could endanger their life [5].

High expenses, and high money loss can result for both businesses and individuals in case of attacks against the data security which can lead to the damaging of devices or stealing

of financial resources. We can see this in the cases related to the smart appliances attacks, the hotel lock system attack, and the stealing of data on passports, which can lead to stealing of goods and financial resources. New measures for protecting against stealing need to be taken, adapted to the current functioning of life in the city. While web cameras in the city and surveillance systems have been installed as part of security, in public places and institutions, and even in personal homes, and while these may discourage thieves to steal in the way they did in the past, new ways of stealing have been devised, using the very high technology that has helped discourage old forms of stealing. Even webcams are not present exactly everywhere, and pickpockets are still around, however. Security is never a solved issue, but an ongoing issue which is constantly in need for solutions.

The fact that a smart city's institutions function based on a computerized system can lead to issues which can cause an entire city to malfunction. As an example, in 2018, there was a ransomware attack of the computer system of Atlanta's City Hall [6, 7]. The citizens were affected, as they could not pay their water bills, and their tickets for city traffic. The computer system was compromised because of cybercriminals. According to Dean (2019), Atlanta is just one example of case of "ransomware against local governments". We can, therefore, notice several cases of this type, including the Baltimore ransomware attack, which occurred in 2019, once again targeting a large city in the USA, just like the Atlanta case. This could be seen as a sign of a frequently occurring problem, which needed attention. In the Baltimore ransomware attack, the following consequences were visible in the citizens' everyday life, which was functioning through a heavy use of high technology first of all, property transfer on the real estate market could not be operated, since the digital system had been shut donw, and the card payment system of the city was not functioning [8]. Neither was the debt checking application. City employees had to start creating Gmail accounts in order to use email sercices, as their email system was not working. However, the newly created Gmail accounts were blocked since so many new account had been created in such a short period of time. Therefore, they could not use Gmail either [9].

The activity in the smart city at public and personal level can, therefore, be hindered due to the data security attacks. Once we are so dependent on technology and computerized systems for government in the city and its used in institutions, we become all the more vulnerable in front of cyberattacks. The cyberattacks can, practically, stop all the normal course of activity and life in a smart city. Next to this immediate inconvenience, we can also expect personal data to be taken illegally and for the citizens to lose even more, especially money from their various cards and accounts.

Source [10] sums up the problem with attacks against data security in smart cities as being related to issues of trust of citizens and to the hindering of the efficiency of the entire technologically-based system, to the point where the smart cities are prevented from "the achievement of their full potential".

Source [11] devised a grid which can be used for analyzing cultures, which was called culture identity manifestations and which included the following categories of elements: traditions, rituals, practices, values, symbols, and personalities. We can fit in within this grid any culture, belonging to any country, as well as subcultures, and cultures which are

created based on supranational organizations and their instilled rules, norms, conventions, laws, and ideologically imposed lifestyle and values. From this point of view, once we understand culture as "patterns of thinking and doing" [11], then we can apply the culture identity manifestations grid to urban life and consider it a culture in its own right. The entire organization of the smart city can be seen as a reproduction of the culture identity manifestations grid.

Regarding values, we can include, as common concerns for people living in smart cities and for governments, together with the policies present at the level of supranational organizations such as the European Union, environmental care, transparent governance, citizens' involvement in political and social life, creativity, open-mindedness, social cohesion, etc. Security and trust regarding usage of data can also be considered a value. Among the symbols, we can include the recycling symbols, together with technology itself, symbolized through QR codes that can be scanned and by smartphones.

Fig. 2 shows an outline of categories based on which we can identify culture identity manifestations, regarding everyday life in smart cities, some of which were already mentioned:

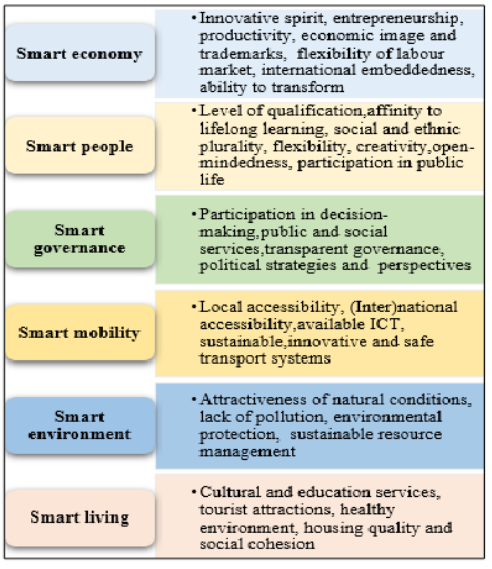

Fig. 2. Aspects of life in smart cities.
Source: [11], *shown in* [4]

We can look at the six axes which have been defined and used by [11] "to measure whether a Smart City is well-performing," and which consider the following dimensions: "Smart economy, Smart people, Smart governance, Smart mobility, Smart environment, and Smart living" [4], and identify culture identity manifestations in a smart city.

These axes include descriptions from where we can identify values which are further reinforced through rituals, traditions and practices, on special occasions, which may include pedestrian street events, where citizens are presented with cultural events samples,

under the form of street shows, e.g. acrobatics, circus elements, magic shows, theatre scenes, dancing scenes, presentations of contemporary artists showing their pantings in the street, street musicians performing live and offering their music CDs, as well as actitivities organized in parks during weekends where walking and using electric or usual scooters and bicycles are encouraged, fairs with handmade objects, natural and bio foods which are encouraged by European Union health policies, book fairs, etc. As far as environmental care is concerned, paying by credit card, and using less cash is encouraged, together with paying various taxes online and not receiving the invoice in print format by postal services. Less bureaucracy means less paper wasted, and more trees present, which can be made available through the digitalization of archives and through computerized systems. However, the security of all these practices and of all the infrastructure and organization of a smart city rely on a fundamental value, which should itself be reinforced through rituals, traditions, and practices, namely data security. Data security is ensured, at supranational level, through the General Data Protection Regulation (GDPR) established by the European Union, and which ensures privacy and individuals' image protection regarding sensitive data. Still, smart cities need to consider the security of personal data, as much as data that is related to the organization of the city by the government and various services, since they have proved in some cases to be vulnerable to cyberattacks. GDPR can be considered both a value and a practice, or a value that is reinforced through the practices represented by policies set up by the European Union.

Once data security is ensured, we can ensure trust of citizens in the authorities, which is always an important element for ensuring stability in the life of the city. As citizens, we project, psychologically, the role we ascribed to parents in our childhoods, namely that of a protector and of someone we trust. We expect protection and trust from leaders, and we are deceived and even angry if they do not comply with this role. Our childhood experiences shape our further relationship with the others, this time extended at the level of society. We can consider Freud's theory of infantile sexuality [12] and various fixations due to issues encountered during our psychological development. Once we have a more pronounced issue with authority, related to trust, it will resurface from childhood to maturity. In addition to psychological expectations, we have expectations created by ethics and conventions, as well as rules and laws, which ask of leaders to fulfill their duty towards the citizens.

Anthropology can explain the role of the leader as related to status, which can be understood as having "a position in a particular pattern," or as "a collection of rights and duties" ([13], mentioned in [14]). Expectations result from the rights, as well as duties, associated with the leader [14]. We deal, when it comes to a leader, with a role expected of him, therefore, and this role can be extended to the smart city itself. Ensuring data security can be associated by citizens with both government, with particular leaders and figures of authority, which can be included in the category of personalities from the culture identity manifestations grid, and with the smart city itself, which becomes itself a projection of the protective role of leaders and of stability of life, meaning ensuring data protection.

With the growing individualism [15] we expect to have ensured our personal space as individuals and to have data security ensured as well, as it can be considered part of our own, personal interest.

Today's mindset makes us willing to protect our personal data, as it is considered a part of our personal space. Everything is regulated through policies and rules, which legitimize these needs.

Additionally, as human beings we have the capacity to imagine and create preventive scenarios. One such hypothetical scenario with repsect to attacks against data security in smart cities is the one related to damaging the function of the traffic. The traffic lights are programmed and once cyberattacks occur, the entire traffic and life in the city could be disturbed, to the point where everyday life activity may no longer pe possible. This has far-reaching consequences, as institutions may not do their work properly once staff members are blocked in traffic, and public life may suffer. Public life has a strong influence on the way the city functions overall, which can disturb the routine and postpone certain activities and processes.

Smart transport system [16] may appear comfortable, and easy to use and operate, yet the danger comes when dealing with cyberattacks as well. We can consider the scenario in parallel with the way in which there is an accident in the city, or any deviation, traffic is delayed. Everything moves slower, and eventually all activity is going to be late.

3. Results

The following results can be identified as a consequence of the present research, and summed up as follows:

- Computerized systems can make some processes in public life in smart cities faster, yet they also expose the functioning of our everyday life to vulnerabilities related to data protection;
- Computerized systems can both ensure stability and instability in the city, function of whether they are not attacked or are attacked;
- Repeated cases of data security attack in similar situations may lessen the trust of citizens in government representatives and in leaders at the level of smart cities;
- Once citizens are no longer trusting authorities, then rebellion and protests can occur, which can destabilize life in the city even more than cyberattacks, to the point where usual activity can beak the natural flow of life activities in the smart city.

Smart cites can lead through the possibility actual actions to stable or unstable conditions. Once activity is delayed in smart cities, insability can can occur, as the natural course of everyday life may have included certain activities which, once postponed or cancelled, can disrupt the usual and expected routine, to the point where some activities can depend on others. In this latter case, the delays may depend on others delays, and entire segments of activities can be delayed. It all depends how urgent some actions are.

4. Discussion and Conclusions

The digital divide in the European Union is one of the frequently discussed topics. This refers to personal possibilities and access to technology, as well as to services that are publicly ensured. A smart city can ensure all these possibilities for its citizens, through providing public access to certain services. Once access to certain services is delayed, the entire city life and activity can be disturbed. It also depends on how soon certain actions can be retaken and on the extent to which activity can return back to normal. The frequence with which attacks occur can also establish the extent to which activities in the city can occur, namely their pace.

Smart cities bring along hopes for the better, as well as expected risks and threats to the stability of everyday life. Ensuring data security can mean a step further. Having citizens trust the leaders of the smart city also ensures harmony and efficiency in managing smart cities. Technology, as high as it can be, means that it is used by human beings, who need to be efficient in their jobs.

Examining previous real life cases and hypothetical scenarios previously discussed or imagined can create a basis for discussion and for reference regarding previous knowledge.

We can cooperate with technology, yet we can never consider it the final solution to our problems.

References

[1] C. Yin, et al., „A literature survey on smart cities," *Science China. Information Sciences,* vol. 58, nr. 10, pp. 1-18, 2015.

[2] K. Davis, „The urbanization of the human population," în *Menard S. W., Moen E. W., Perspectives on Population: an Introduction to Concepts and Issues*, Oxford University Press, 1987, pp. 322-330.

[3] R. P. Dameri, et al., „Searching for smart city definition: a comprehensive proposal," *International Journal of computers & technology,* vol. 11, nr. 5, pp. 2544-2551, 2013.

[4] S. Ouidad și T. Mazri, „Smart City Security Issues: The Main Attacks and Countermeasures," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences,* vol. 46, pp. 465-472, 2021.

[5] D. Popescul și L. D. Radu, „Data security in smart cities: challenges and solutions," *Informatica Economică,* vol. 20, nr. 1, 2016.

[6] G. Falco, et al, „A master attack methodology for an AI-based automated attack planner for smart cities," *IEEE Access,* vol. 6, pp. 48360-48373, 2018.

[7] C. Lamers, et al., „Ransomware: A Threat to Cyber Smart Cities," în *Cybersecurity for Smart Cities: Practices and Challenges*, Springer International Publishing, 2023, pp. 185-204.

[8] E. Stewart, „Hackers have been holding the city of Baltimore's computers hostage for 2 weeks, Vox," 2019. [Interactiv]. Available: https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers.

[9] C. Lecher, „Google shut out Baltimore officials using Gmail after ransomware attack, The Verge," 2019. [Interactiv]. Available: https://www.theverge.com/2019/5/23/18637638/google-gmail-baltimore-ransomware-attacks.

[10] N. Neshenko, E. Bou-Harb și B. Furht, „Cyber Brittleness of Smart Cities," în *Smart Cities: Cyber Situational Awareness to Support Decision Making*, Springer International Publishing, 2022, pp. 19-40.

[11] S. Baciu, Culture: An Awareness-Raising Approach, Bucharest, Romania: Cavallioti Publishing House, 2012.

[12] S. Freud, Three essays on the theory of sexuality: The 1905 edition, Verso Books, 2017.

[13] R. Linton, The study of man: An introduction, 1936.

[14] G. Lang, „The Concepts of Status and Role in Anthropology: Their Definition and Use," *The American Catholic Sociological Review*, vol. 17, nr. 3, 1956.

[15] H. C. Santos, M. E. Varnum și I. Grossmann, „Global increases in individualism," *Psychological science*, vol. 28, nr. 9, pp. 1228-1239, 2017.

[16] R. I. Meneguette, R. De Grande și A. A. Loureiro, „Intelligent transport system in smart cities," *Springer International Publishing*, 2018.