The Security of Portugal Smart Cities: Vulnerabilities, Risks and Prevention

Gabriel Lima

University Lusófona from Porto, Portugal

gabrielfariali@hotmail.com

Abstract. In the current age, it is noticeable that the evolution of modern society leans towards faster and simpler ways of doing any type of daily task, in that sense, it would not be too late to introduce the concept of Smart Cities, a city with improved networks and services like public transport, water storage, light, and efficient administrative services are optimal as possible with the use of digital and telecommunications technologies for the benefit of its inhabitants and internal businesses. But smart cities are quite a double-edged sword topic as they can provide effective and efficient delivery of services, yet they can create new vulnerabilities and threats, possibly making the city insecure and open to several forms of criminal activity. In this study, we aim to examine this technology in Portugal and go deeper into this mostly forgotten topic about the insecurities concerning smart cities, specifying the risks that the country can currently face due to not considering security tests of new technologies and not granting the full protection of this huge communication. In the common sense that any city can start investing in this kind of environment, is only logical that the security has to be directly proportional in terms of investment, in this sense this paper also aims to expose existing forms of strategies to prevent (Strategies like awareness regarding cybercrimes is pivotal for tackling and preventing cybercrimes, factors such as social media, government initiative and organizations play a huge role in preventing any of these cybercrimes) or deal (formation of core security and computer emergency response teams, a change in procurement procedures, and continuing professional development) with any type of security tribulation.

Keywords: Portugal, Cyberattack, Risk, Security, Smart Cities, Urban Resilience, Prevention, Vulnerabilities, Social Engineering, Digital Services.

1 Introduction

The concept of the "smart city" has experienced a considerable increase in studies and analyses in academic or industrial fields. The promise of solving and optimizing everyday problems encourages cities to take an interest in this new type of environment. According to a study by United Nations in 2014, more than half of the world's population now lives in urban areas, and the trend is rising, with forecasts for 2050 already at around approximately 66% [1]. These data do not differ from what is currently happening in Portugal, where the number of people living in urban areas is gradually and continuously increasing [2], as shown in these United Nations graphs.

10.11228/dpsc.03.01.001

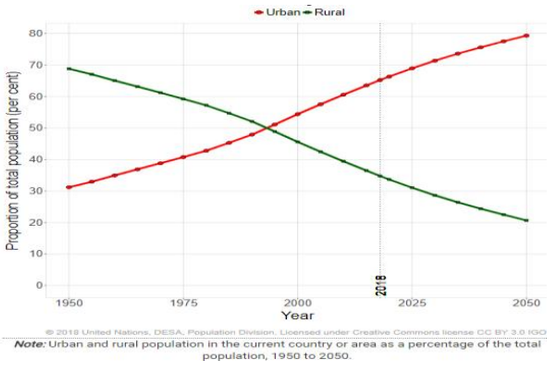

Fig. 1. Percentage of population in urban and rural areas in Portugal.

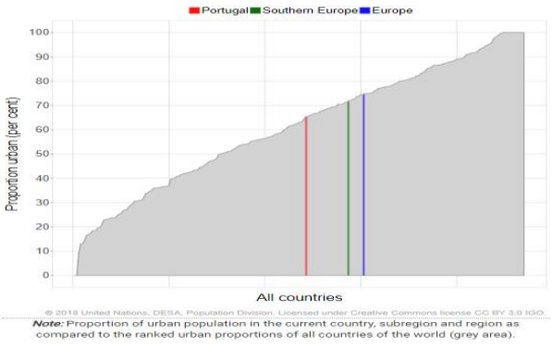

Fig.2 Percentage urban by country in 2018.

This population increase certainly brings with it new social challenges, such as the inability to provide the entire population with the necessary supplies, increased waste, and, as a result, flooding, or health problems. The problems certainly even affect the environment around an inhabited city [3]. Just as urban population growth, developments in the world of technology have not stopped growing, it did not take long for the idea of a technology network to emerge that can provide effective, rapid, and practical solutions for managing any area where this is required, so a "smart city" emerges when a deficiency or insecurity in the social sphere is effectively addressed, with the aim of alleviating the challenges and improving the well-being of a citizen; in addition to addressing current problems, a smart city has an incredible potential for expansion and can intelligently support economic, environmental and social developments. Following the same line of thought, one can imagine the creation of many new, "smart" ways of tackling everyday problems, such as a smart transport system, a smart government system, a smart health system, a smart environment system, a smart transport system or even smart houses and buildings. According to IDC, investment in smart city initiatives is growing exponentially [4], and we can imagine why hundreds of cities are interested in such an effective tool for urban development and management.

1.1 Paradox in smart cities.

Like any kind of new technology, the promises of utility and exclusivity is always of enormous interest to the large population, the same, many times is not interested in the in-depth analysis of new technology and not realize what it can accept in your personal life. The process of adapting to a new technology brings with it a series of innumerable problems related to security, even more so when this technology is a complicated architecture of networks and intelligent systems that can and should involve an entire city, there are frequent attacks on intelligent systems on a daily basis, such as unauthorized access or denial of service (Dos). Since the attempt to build an intelligent electricity system, there have been unprecedented attacks, such as the failure of the power supply in Ukraine in 2015 due to hacker attacks [5], cases of excessive data collection by service providers that pose a threat to privacy [6], or Russian attacks on the US electricity system. In discussing the term cyber-attacks, the energy secretary Rick Perry says that "literally hundreds of thousands of times a day" [7 . Such a statement puts into perspective the great para-doxia of smart cities, a promising and visionary environment in which problems with energy, transportation, water, or government administration can be solved as simply and easily as possible, but few analyze or worry about the great security risk associated with such a system.

There is a fine line between promoting the well-being of society through technology and opening up new risks and vulnerabilities for it. This paper attempts to explore this relationship between risks and benefits by examining the already documented and observed risks posed by this system, attaching importance to the extent of vulnerabilities that allow threats to violate and denigrate the level of integrity, confidentiality, and availability of the system, and also looking at the preventions that can be taken in the search for a safer future. all these topics will be covered below in Chapters 2 and 3.

2 Risks and Vulnerabilities of Smart City

A critical analysis of the history of mankind shows us an important fact: with the constant progress of technology, some seek or simply find ways to attack, penetrate, corrupt, or cheat the virtual environment. These attacks can be the fruit of malicious intent with some kind of personal interest or oversight that was carried out without any idea of possible subsequent events [8]. Smart Cities are no different from these because the size of their system covers a surprising range of vulnerabilities and risks; the most promising problems of a smart city are related to a system failure due to attacks or malfunctioning of the system, or to a large scale data breach [9]; it is noteworthy that this type of system combines several characteristics that make it vulnerable, the process of centralization and integration of technologies, coupled with a full Internet connexion, makes this system a major potential target for attackers who could access this network and cause damage on a large scale. One factor that should be noted is the fact that Ukraine has in the past experienced terrible episodes of total power loss [5]. It is inevitable to make a comparison that an attack of this magnitude was not possible in ancient times, and we can still say that we are increasingly moving towards having vital infrastructures in our society that are potentially vulnerable to a series of new attacks, even

worse given the fact that, because of the time we live in, these attacks can be commanded by people all over the world, as was the case with the Russian cyber-attacks on the United States, which were also mentioned earlier. All these attacks are living proof of the risks to which we are exposed as a society, bearing in mind that the introduction of an intelligent system is inevitable over the years, which demonstrates, even more, how important analyses, studies, preventive measures, and the whole process of cybersecurity are today and even more so in our daily lives.

According to Shirey and the Internet Security Glossary, the threats that a system can face are divided into four categories: Attack on the correct operation of a system (disruption), inducing error (deception), unauthorized access to information (disclosure), and usurpation [10]. These categories can be characterized as follows [11]:

- Disruption is defined by the corruption or degradation of systems that have a negative impact on the services offered; this situation usually occurs when the system component to which the information is delivered is directly disabled or when the system is requested to transmit contaminated data.
- Deception is described by the deliberate effort to deceive different entities. For example, a vengeful entity may send false or inaccurate data to another person in the belief that the data is correct. Fake entities can be used to incriminate others or gain unlawful access.
- Disclosure is characterized as gaining unauthorized access to secure data. Delicate information could be wrongly presented to unauthorized elements or could be obtained by an attacker who circumvents the security precautions of the framework.
- By usurpation an attacker can gain unauthorized control over a system. This unauthorized control may allow the attacker to illegally gain access to secured information or services or to disrupt the framework itself to cause false or malicious behavior.

It is also important to identify that the vulnerabilities of a system are usually originated by common and major failures, such as:

- Poor design: Systems are created with security holes.
- Poor implementation: Systems are incorrectly configured and therefore vulnerable to attacks.
- Poor management: The testing procedures are inadequate, or insufficient or both. Security measures may not have the support, documentation and monitoring necessary for the correct functioning of the system.
- Physical means: The physical installation is not adequate and consequently the physical protection of equipment is compromised, every system is vulnerable to unforeseen situations and human failures and these can range from sloppiness, laziness to greed or some personal revolt.

In this paper we try to highlight the two main risk areas in a Smart City, focusing on attacks that directly affect system availability, integrity and also confidentiality.

2.1 Attacks on confidentiality level, Data Breaches

The nature of a smart city is the connection of objects present in your network to provide continuous communication and dynamic services, this interconnection is ensured through various objects and in various areas in our daily lives, we can cite as an example the so present Embedded System such as smartphones, TVs, printers or as many other specific engineering devices. Besides common embedded systems, there is a range of objects that are not taken into account such as clocks, household appliances, sensors that can be used to monitor any type of information desired, doors, bridges for education. In this way Smart cities are directly involved in data collection, intensive analysis, and storage of tons and tons of data each one of them related to an entity of the society, information that is sensitive and valuable that we almost never realize of yielding to a platform of the government, what can happen as well is the very terms of conditions request the freedom to be as evasive as they want like sharing the data with danger third parties if the user allows it unnoticed.

We can adopt an even more pessimistic view of the scenario, an intelligent system that could monitor each of an individual's actions, storing and analyzing data to build a profile linked to them. If this profile, loaded with sensitive information, is in some way intentionally or unintentionally leaked or stolen due to some exploitation of the vulnerabilities and risks of the system, this would pose an unprecedented threat to the individual in question. The attacker could then have access to the individual's location and monitor each of his or her steps, knowing the right times to commit robbery or even assault against the individual. Furthermore, we are still at risk of being the target of a deception attack, that is, the attacker uses the data in an unauthorized way to steal the information he wants, it is possible to realize that the information leads to knowledge and the knowledge leads to power, that is, by obtaining this data, an attacker has countless ways of taking advantage of it and benefiting himself consequently affecting those who own the data.

According to DLA Piper survey, in Europe over 59,000 personal data breaches were reported [12], and the International Data Corporation predicts that by 2020, a quarter of the world's population will have been affected by a data breach [13]. In Portugal we have reports and analyses according to the International Network of Privacy Law Professionals that show a severe lack of concern with the information collected [14], resulting in fines that will need to be paid to GDPR.

Despite the great risks involved in data collection, one thing is certain, the analysis and collection of this information will allow the emergence of an intelligent model that can deliver all the intended benefits. Even in a non-smart city environment, where many Portuguese citizens use their smartphones for trivial things like checking the climate, they are benefiting from this vast network of data collection, The purpose of this paper is not to condemn this practice, which has already been adopted, because it would be impossible, but to focus on imposing limits when a data collection is something profitable and good for the urban development of all or when a collection is compulsive and

directly affects the most valuable asset of society, namely its own people, whose privileges are attacked and whose identities are stolen in exchange for a set of data. This kind of practice can evolve even more if we think of a world where all the data we use is organized and archived, this betrays a huge policy of fear of the people in relation to the government, where the government could have all the knowledge possible and consequently manipulate the mass for its own benefit without it noticing it, while the people would know the minimum due to the lack of transparency of the system, as a final result democracy itself and individual freedom of choice could be affected directly with the excessive date breach as we can see current examples such as [15] and [16] where many of the technologies that are frequently associated with smart cities have been used to create a surveillance state, where the people can no longer practice their religion openly or assert the individual freedoms that we take for granted.

A complete survey [17] suggested that four sources of facts can be used to hack privacy, namely, observable data, repurposed data, published data, and leaked data, which carries a giant quantity of users' touchy information. Sometimes, the privateness of residents can be breached even although a device is tightly closed and not harmed through offenders. One practicable way for this to occur is the effective data mining algorithms. With these mining tools, some service providers and third events can easily discover consumers' private information, for example, the example provided by [18]. Besides this tool, we also have an attack to which we are all exposed, the attacks of social engineering. These attacks correspond to a large part of the threat and risk to smart cities, both in data breaches and attacks against the availability of the system. The criminals who use this technique try to deceive the user so that they can perform actions that will cause great failures in the information security system, the damages, and causes of this strategy can vary according to the profile of the attacker and his objective, it can be just a form of trot to get sensitive data in an easy way or assuming an extremely greater magnitude with the possible corruption and disruption of public transportation systems, so it is possible to cause serious accidents, the city's water system could be damaged, as well as its nuclear plants or any other type of installation that will always be of extreme importance for the social good of the population. A common and long-standing form of attack on the system's confidentiality using social engineering resources would be phishing attacks, which means, targeting email users to capture the user's credentials. Hackers can use the information gained to access smart city systems for malicious purposes. The techniques and technologies behind phishing will continue to evolve [19]. The graphic below shows the number of data breaches in Europe according to [12] and we can see how Portugal is dealing with the situation in data breaches in relation to other neighboring countries, taking into account that the population difference plays a big role in a possible comparison of situations.

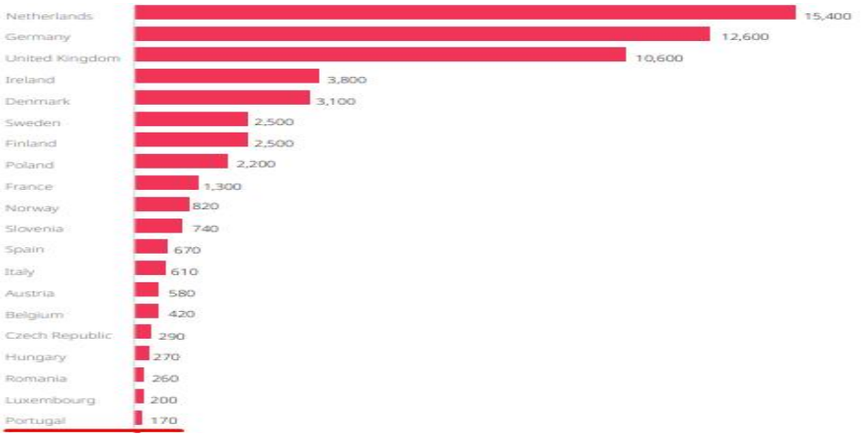

Fig. 3. Number of data breaches notified from May 25,2018 to January 28,2019

2.2 Attacks on Availability and integrity level

The most effective way to compromise the complex network of a smart city is through cyber-attacks that seek [19]. As soon as a device is compromised as a result of an attack, its whole set becomes vulnerable for any type of next attempt, these compromises or cyber-attacks are imminent threats to any type of smart city, as already discussed there are a series of risks and vulnerabilities to be exploited by attackers, one of these threats that would seek to interrupt the correct functioning of a system, denying its service of use to the population would be threats against the vulnerable points of the SCADA (Supervisory control and data acquisition) system.

SCADA. It is a system that controls functions and workflows of various urban infrastructures, we can highlight the electrics grid, water supply, and traffic control, all these rely on real-time analysis that the SCADA system provides in addition to automated services for changing settings in your system, requiring human intervention only in special cases. It is expected that a system of such importance in the daily life of any smart city will have to be well protected for the good of the population, in practice what we find is that supervisory systems of control and data acquisition can be tracked since the year 1920 [20] and as consequence many of these systems are now outdated in the face of the reality of computer evolution and consequently the evolution of cyber-attacks.

Severe SCADA systems have already been compromised, [8], [20], [25],[28] where their attackers alter the performance of urban structures and cause the population to cease using the service. In 2014 a study [21] showed that out of a total of 599 security executives from utility, oil and gas, energy and manufacturing companies, almost 70% recorded at least one security breach that led to the disruption of the performance of these infrastructures, moreover when asked about the probability of future attacks on ICS organizations or SCADAS systems, 78% of state security officials say that a

successful attack on the security of organizations is expected in the next two. These studies are frightening news given that these industries play a large role in a global economy and could in no way be such easy targets for an attack to degrade the system.

There are infrastructures that will certainly have more impact when compromised by some kind of attack, we can cite two very important ones that would be the electric network of a city and the management system of transport and vehicles.

Attacks on the electricity grid. Events of attacks against the availability of electricity grids around the world [5], [7] have already been discussed in this paper; these grids use the SCADA system to generate, transmit and distribute electricity in a monitored and controlled manner [20], and are therefore a major target for attackers because of the magnitude of services this infrastructure provides to the population of a city. These power grids have been present for a long time in large spots, so it is not strange to hide outdated systems in their security and prevention levels, so the current level of daily attacks on power grids increases considerably [20] and ways are increasingly being found to compromise all this infrastructure with low-cost tools [22], [23] increasing the fear of a "smart" future.

Attacks on Transport management systems and vehicles. Just like electricity networks, attacks against the transportation management system are also extremely common and this tendency to attack continues to increase with the arrival of new attackers and new discoveries made by them, so studies and news also emerge frightening in relation to existing attacks and concerns, we have as example situations where attackers managed to stop the main street for 8 hours causing a great disturbance in traffic [24]. Like any technology, these cyber-attacks also seek to evolve and learn the most realistic and effective way possible in their attacks, so we can have access to studies that show hundreds of traffic lights having their service of use denied by just a laptop and a wireless radio [25], there are already cases that stir up the fear of an attacker being able to attack a system from anywhere in the world [26] or cases where passengers on the edge of a train were injured due to a breach of security made by a teenager [23], [27]. But these attacks are not only exclusive to public transportation in a city, any vehicle today also has total vulnerability to some kind of disruption to its system, as we know a modern car can contain numerous sensors connected to various control units that in turn connect to wireless networks.

It has already been observed attackers taking advantage of this knowledge [28], taking control of the entire internal computer network of a vehicle, being able even to cut the physical control of the citizen in his own car and assuming it remotely and completely, thus being able to practice any act of evil against the individual attacked.

3 Possible preventions

A common factor observed in history is that since the appearance of belongings and interests, those who are in charge of identifying and exposing vulnerabilities to

get these interests also appear. With all the time any kind of security, sophisticated or innovative will inevitably be the target of a defeat against a determined attacker, every security system already starts from an evident disadvantage knowing that the main advantage of the attacker is that he only needs to find a single weakness, while the administrator must find and eliminate all the weak points to achieve perfect security, it is thus given the need to adopt certain practices in search of mitigations and controls throughout this gloomy scenario presented.

Two types of key risks need some mitigation process, one would be the process of ensuring a good design and a good implementation of the system, with new technologies that are implemented in this vast network or possible "smart" upgrades to existing urban infrastructures, and the second would be the process of mitigation of data generated, stored and shared through this vast network, i.e. data breaches.

When we analyze the means of mitigation, we can see that they can arise from two main points, they can be measures adopted in the scope of the market presence in the system or they can be measures adopted in the scope of the government itself as an entity that has powers, rights, and duties and also seeks to mitigate as much as possible any adverse situation to the welfare of society.

As discussed previously in the two key types of risk and also the most common origins of vulnerabilities in a system, an approach made at the level of the market of a smart city has to start from security by design, with each new implementation of a smart city system it is necessary to guarantee levels of protection to preserve the well-being of the society, these levels refer to:

- Transparency with citizens
- Accountability
- Anonymity and security measures
- Cyber defense services appropriate and always updated
- Standards, practices and regulations of safety and use

Making this practice something immutable over the years, software companies could then help each other with the creation of thorough and rigorous standards in the area of security, as well as the creation of good practices that could thus put the team of defense against cyber-attacks in a fair fight with the incredible evolution of the means of attack over the years, after all, the best way to prevent risks from happening is not to create vulnerabilities in the first place.

With this kind of thinking where each company practices constant self-evaluation and also encourages others to do the same, security becomes more and more necessary and of fundamental importance in any new addition to the great network system in a smart city, making companies that don't adopt this method look bad in the public eye, bringing a competition that any business wouldn't want to be behind.

The measures adopted by the government should also always seek to guarantee the levels of quality in protection, an example of a measure to be adopted and perhaps the most important in the field of data breaches would be information open to all citizens of a smart site about how data collections happen and how they are used, a transparent system will always bring more comfort and security. The best possible scenario for a citizen would be the personalized privacy of their data in the best

possible way and still be possible the effective use of the functionalities of a smart city and this is the thinking that would replace the current thinking of the bigger the data collection the better [29]. Mitigations methods are not complete without a damage assessment plan, any system is subject to attacks so every system must be equipped with maneuvers to minimize the damage that has occurred, a zeal for data begins with storing it on various platforms and "safes" capable of storing the information in cyclical periods and can serve as the decisive tool for data recovery when needed.

Even the best mitigation strategy and effective prevention would not be able to eliminate all the vulnerabilities and risks associated with a smart city environment, in the search for the evolution of security, several mechanisms were developed to protect the levels of availability, integrity, and confidentiality of the systems but in the direct application of these mechanisms there were always failures, This is due to the same reasons of prevention in marketing levels, the mechanisms launched do not pass through any standard of quality customized for the environment of a smart city, such as the numerous sensors scattered in this system do not have the processing power necessary to accommodate high-end security mechanisms and because of this can only be configured with weak encryption systems being a huge risk for the entire structure.

Currently, all new mechanisms intend to follow the trend line of the new technologies, that is, they need to be more and more practical, flexible, dynamic, and low cost for the mass acquisition by some entity, the concern and the best investment in this current framework would be the deeper research in ways to guarantee all these qualities to the simplest sensor, while the necessary levels of protection are guaranteed, beating against security by design being one of the best practices to adopt.

Unfortunately, according to the current picture, the threats faced and the future fears it is fair to conclude that more effective forms of protection, prevention, and mitigation need to be developed to keep pace with the great growth of attacks and the "smart city" concept, this kind of thinking where security has its place is the best chance of new opportunities and new frameworks within such a huge and dangerous technological environment.

4 Conclusion

In this paper we can go deeper into the current state of security in a smart city environment in Portugal, we can clearly analyze the duality of this system that promotes a basis for the creation of a new social architecture allowing environments that support an undefended number of computer protocols occur simultaneously for the welfare of society, despite the benefits that smart cities bring, also create new risks and in unimaginable degrees opening up forms of vandalism, disruption, and criminal exploitation.

It is noticeable how the development of new methods and models of protection is essential and in great demand, because it is a challenge of magnitude above the communitarian, and because of that this paper also seeks to discuss the current problems in companies and in bigger entities like the government about new approaches and

strategies of adoption benefitting the general welfare such as security-by-design and the continuous improvement from the adoption of the protocols of good practices being done by all the elements that compose this system, This adoption process should be taken with a regulatory approach for entities that have a higher risk and consequently higher side effects involved with their system, thus being able to be transparently monitored to the public and guaranteed compliance with the suggested standards.

Evidently we cannot stop the evolution process that directs these systems, but it is not yet late to analyze how we will make this transition and how we will ensure total control and use of it, currently, values are inverted and not given due importance to issues that really matter such as the extent of security and vulnerabilities.

With the forms of prevention discussed in-depth and maneuvers that would promote an incredible advance in the current situation, it is possible to have smart cities that only offer optimized services and a better quality of life without the blatant concern of the greatest risks of privacy and security, as long as more and more importance is given to the security and privacy of the citizens, with the several rigorous criteria being applied to each stage of the development of a system of this magnitude, it is possible to believe that someday we will have this new help that technology would bring to the daily life of each one of us, in the current and future days.

References

1. U. Nations, "World urbanization prospects: The 2014 revision, highlights. Department of economic and social affairs," Population Division, United Nations, 2014.
2. Macrotrends Portugal Urban Population Page, https://www.macrotrends.net/countries/PRT/portugal/urban-population, 2018, last accessed 2020/11/22
3. National Geographic urban threats, https://www.nationalgeographic.com/environment/habitats/urban-threats/, 2020, last accessed 2020/11/22
4. IDC's Worldwide Smart Cities Spending Guide page, https://www.idc.com/getdoc.jsp?containerId=prUS46016320,2020, last accessed 2020/11/22.
5. Author, F.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010).
6. Humans Rights Watch, "How Mass Surveillance Works in Xinjiang, China", https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang, 2019, last accessed 2016/11/21.
7. Rick perry, "Energy and water development appropriations for 2019",https://www.govinfo.gov/content/pkg/CHRG-115hhrg32414/pdf/CHRG-115hhrg32414.pdf, 2019, pp 140, , last accessed 2021/01/12.
8. NATO review magazine "The history of cyber attacks – a timeline", https://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm, 2013, last accessed 2020/11/24
9. Josh Lake, Comparitech "Smart Cities, Cybersecurity and privacy: What are the risks", 2019
10. Shirey R RFC 2828: Internet Security Glossary, http://www.ietf.org/rfc/rfc2828.txt, 2000, last accessed 2020/11/22
11. Journal of Internet Services and Applications, "Virtual network security: threats, countermeasures, and challenges", 2015

12. DLA Piper GDPR data breach survey:, https://www.dlapiper.com/pt/portugal/news/2019/02/dla-piper-gdpr-data-breach-survey/, February 2019, last accessed 2020/11/24
13. International Data Corporation, https://www.csoonline.com/article/3014493/data-breaches-will-affect-14-of-the-worlds-population-by-2020-idc-predicts.html, 2015, last accessed 2020/11/24
14. INPLP, "Portugal: Recent fines for the breach of the GDPR", https://inplp.com/latest-news/article/portugal-recent-fines-for-the-breach-of-the-gdpr/, 2019, last accessed 2020/11/25
15. The new York times, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html, 2019, last accessed 2020/12/03
16. The new York times, "China Is Detaining Muslims in Vast Numbers. The Goal: 'Transformation.'", https://www.nytimes.com/2018/09/08/world/asia/china-uighur-muslim-detention-camp.html, 2018, last accessed 2020/12/03
17. K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEE, https://ieeexplore.ieee.org/abstract/document/7823349, 2017, last accessed 2021/01/12.
18. L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176, https://ieeexplore.ieee.org/abstract/document/6919256, 2014, last accessed 2021/01/12.
19. Oliviah Nelson, Cyber Experts "Smart city security", https://cyberexperts.com/smart-city-security/, 2019, last accessed 2020/12/03
20. The Center for the Study of the Presidency and Congress (2014) Securing the U.S. Electric Grid.WashingtonDC.https://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf, 2013, last accessed 2020/12/05
21. Security Week: "Unisys & Ponemon Institute 2014 Survey".
22. Krebs FBI: Smart Meter Hacks Likely to Spread, April 9th, Krebs on Security, 2012.
23. Nanni, G. Transformational 'smart cities': cyber security and resilience. Symantec, Mountain View, CA, 2013
24. Paganini, P. Israeli Road Control System hacked, caused Traffic jam on Haifa Highway. Hacker News, http://www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf, 2013, last accessed 2020/12/06
25. Leitner, T. and Capitanini, L. New Hacking Threat Could Impact Traffic Systems. NBC Chicago, http://www.nbcchicago.com/investigations/series/inside-the-new-hacking-threat/New-Hacking-Threat-Could-Impact-Traffic-Systems-282235431.html, 2014, last accessed 2020/12/06
26. Cerrudo, C. Hacking US (and UK, Australia, France, etc.) Traffic Control Systems, IOActive Blog, http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html, April 30th 2014, last accessed 2020/12/06
27. Goodman, M. Future Crimes: A Journey to the Dark Side of Technology – and How to Survive It. Bantam Press, New York, 2015.
28. Greenburg, AHackers Remotely Kill a Jeep on the Highway—With Me in It. Wired 21st July 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, last accessed 2020/12/06
29. K. Xu, Y. Qu, and K. Yang, "A tutorial on the internet of things: From a heterogeneous network integration perspective," IEEE Network, vol. 30, no. 2, pp. 102–108, https://ieeexplore.ieee.org/abstract/document/7437031, 2016, last accessed 2021/01/12.