Assessing the gamification approach on EU's critical infrastructure security[1]

Ana Maria COSTEA, PhD

National University of Political Studies and Public Administration (SNSPA)

Abstract:

The present article aims to tackle the issue of gamification of smart cities from a cyber-security point of view. More specifically, the analysis is going to focus on the transportation sector and its effects over the security of the individuals, economic operators and states. Firstly, the article is going explain the concepts are being employed throughout the paper like: critical infrastructure, gamification, smart city and Intelligent Transport Systems (ITS). Secondly, the analysis is going to focus on the needs and main benefits that smart cities bring to the life quality of its citizens, thus cause and effect. After establishing the current status quo, the analysis is going highlight the security vulnerabilities that can arise from using ITS and the gamification technics in smart cities especially in the case of IPT since it is part of the critical infrastructure of that state. Taking into consideration the benefits and the costs, the analysis is going to be finalized with recommendations regarding possible ways to reduce the cyber security related costs for transportation gamification at the level of the European Union. In order to be able to develop the recommendations, the following research questions are going to be addressed: Which is the impact of smart cities and gamification in Europe? How should the EU dealing with its cyber-security vulnerabilities especially in the transportation field?

Keywords: critical infrastructure, cyber-security, the European Union, transportation

Introduction

The development of digitalisation and connectivity brought huge benefits for both states and individuals, but also important vulnerabilities in terms of security. One example in this case

[1] The article is part of the development of a study on the application of the game approach in logistics and transport training (Output Title O4) under the Erasmus + strategic partnership project *„Building an innovative network for sharing of best educational practices, incl. game approach, in the area of international logistics and transport“, Project number: KA203 / HE-25 / 13.09.2019*

could be Estonia in 2007, moment when the cyber dimension begun to be perceived as a national security dimension. Regardless of the national level, thus apart from the security of the governmental devices, networks, servers, the technological area brought also the vulnerability of the individuals in front of attacks like DDoS, cyber-phishing, botnets, cyber-bulling, etc. At the same time smart cities brought another layer of vulnerabilities, due to the fact that the critical infrastructure of the city is permanently connected on the internet and as every online system it can be hacked[2]. Following this logic, the EU decision makers decided that “*all necessary actions need to be taken to improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses – ranging from small and medium-sized enterprises (SMEs), as defined in Commission Recommendation 2003/361/EC (4), to operators of critical infrastructure – are better protected from cyber threats.*[3]”(The Cybersecurity Act, 2019). In order to reach this goal they created the European Union Agency for Network and Information Security (ENISA), a European body that was established by Regulation (EU) No 526/2013 of the European Parliament and of the Council[4]. The present article is aimed to tackle to issue of cyber-security of smart cities that employ gamification technics for their transportation sector. Following this aim, there are three research questions are employed: Why do we need smart cities? Which is the impact of smart cities in Europe? How should the EU dealing with its cyber-security vulnerabilities especially in the transportation field? But before answering to these questions, we will analyse the concepts that are going to be applied throughout this paper.

Critical infrastructure

[2] More information can be found at: Council Directive 2008/11/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, specifically Art.2 and Annex I

[3] For more information about the Cybersecurity act please access REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Accessed on 15 August 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[4] For more information about ENISA please access Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013, p. 41).

At the level of the EU, the concept of critical infrastructure is defined as "*an asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a MS as a result of the failure to maintain those functions*." (Article 2a of Directive 2008/114/EC)

From a theoretical point of view, the concept of critical infrastructure was viewed as an essential part of security by the Copenhagen School theoreticians. They viewed security as comprising five different sectors: military, economic, political, environmental and societal[5]. Given the fact that cities became bigger and bigger, that the population living in the urban areas grew and that European states cooperated more and more due to the European project, the critical infrastructure as part of the last type of security became essential in ensuring the local, regional and even national security for a state. Traditional examples in this case could be a bridge that connects two major cities or even countries; the governmental buildings, the electric grid that powers a major city, the train routes, the air traffic, the highways, etc. Nowadays the concept of critical infrastructure changed due to the current technological development especially since the deepening level of cooperation and connectivity have put an emphasis on the transportation sector, field that suffered huge changes over the years. Thus, today we can call as being part of the national/regional/local critical infrastructure new elements like: the internet wires, the computers, the servers, the internet connection and its speed, instruments that ensure the flow of data and its storage, since a large proportion of the activities that were carried out by the government or by the civilians face-to-face moved in the online areas. Individuals can pay their state contributions online, they can even apply for citizenship via online, like it is the case of Estonia. These changes brought huge benefits, but at the same time, they emphasized also major vulnerabilities of the system, as we are going to be highlighted throughout this article.

Gamification

[5] More information about the concept of security from the Copenhagen School point of view can be found Barry Buzan, 1991, People, states, and fear: an agenda for international security studies in the post-cold war era. Boulder, CO: L. Rienner.

In order to make the online systems friendlier, efficient from an economic point of view and at the same time sustainable, the decision makers applied the principles of gamification to services that at the first view did not have a direct connection to games, like for example: e-government, infrastructure, banking system, etc. (Zica, Ionica and Leba, 2018, p. 3). The concept of gamification can be understood as applying the principles of games (like rewards, competition, fun, challenges) to non-game related fields (Zica, Ionica and Leba, 2018, p.3) for different purposes. For example, British and Australian authorities wanted to encourage the population to use more the bicycles or to walk. The results were visible on short term since in Australia 35% of the car trips to school were replaced by eco-friendly and healthy transportation means (Zica, Ionica and Leba, 2018, p.4). Another example can be seen in Singapore were an application with rewards was introduced so that people would start using public transportation in other intervals that the ones that represent the rush hour (Zica, Ionica and Leba, 2018, p.4).

Together with the benefits of having lower costs for its users, but also for the providers and being eco-friendly and sustainable, the integrated systems proved to be vulnerable in front of cyber-attacks. This issue is even more important, since the digitalisation process touched upon the critical infrastructure of the states making it an issue of national security, even a regional and international one if we take into consideration the case the European Union and its four liberties. “*For that reason, it is important to consider security for Intelligent Public Transport to protect the operators, the economy and the life and safety of citizens. However, IPT faces several challenges in this direction: there is currently no EU policy on cyber security for transport, the awareness level is low and it is difficult for operators to dedicate budget to this specific objective of cyber security*” (Lévy-Bencheton and Darra, 2015, p.7).

Smart City and ITS

A smart city should be understood as “*a city that uses ICT [*information and communication technology*] to meet public needs and foster development in a multi-stakeholder environment”* (Lévy-Bencheton and Darra, 2015, p.13).

As defined by the European Commission in the Directive 2010/40/EU of the European Parliament and of the Council on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (2010, 1), Intelligent Transport Systems (ITS) "*are advanced applications which without embodying intelligence as such aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated and 'smarter' use of transport networks*." Another definition refers to "*systems incorporating a wide variety of technologies (telecommunication, IT, automation, measuring) and management techniques applied in transportation for the purpose of protecting the life and health of traffic participants, increasing the effectiveness of the transportation system, and protecting the natural environment with all its resources*" (Stawiarska and Sobczak, 2018, p. 3).

Nowadays Europe hosts around 240 cities that have taken the necessary steps in order to become what are called smart cities and all are using the ITSs. The majority of them are geographically found in Western Europe, particularly in France, Netherlands, Italy, Spain and Austria. As it can be seen below, there are fewer smart cities in Eastern Europe (*Euractiv*, *How many smart cities are there in Europe?*). At the same time their number is high enough all around the EU so that their in/security and their (lack of) efficiency has a potentially large impact over the security of the EU member states and even the region as a whole. This aspect is even more important since, according to the recent studies, "*Europe's level of urbanisation is expected to increase to approximately 83.7% in 2050*" (*European Commission*, *Developments and Forecasts on Continuing Urbanisation*). From this point of view, we could say that a smart city is more than a desirable framework. Rather than that it became a necessary solution for the current dynamics due to the following specific factors:

- The growing number of population in the urban areas. Since the urban centres attracted more and more people to work or the live there, the need for redefining the city's infrastructure arose. Since it would have been very difficult, if not impossible, to construct new infrastructure connections due to the space/geographical limits, the decision makers had to come up with new, innovative methods of making or maintaining the fluidity of the traffic in order to maintain the life quality of the citizens and the economic development of the city.

- The need for sustainable policies. Global warming is an issue for the entire globe. At the same time, it cannot be tackled only at global level, since the actual pollution starts from the local one. In this sense, states, especially the EU member states developed eco-friendly policies in order to protect the environment and to reduce the air pollution. In this sense, they invested in buying electrical cars and use them for the public transportation of people. Another example is represented by the public campaigns to share cars or to use alternative transport methods like public transportation instead of personal cars, trains, bicycles or electrical push scooters.

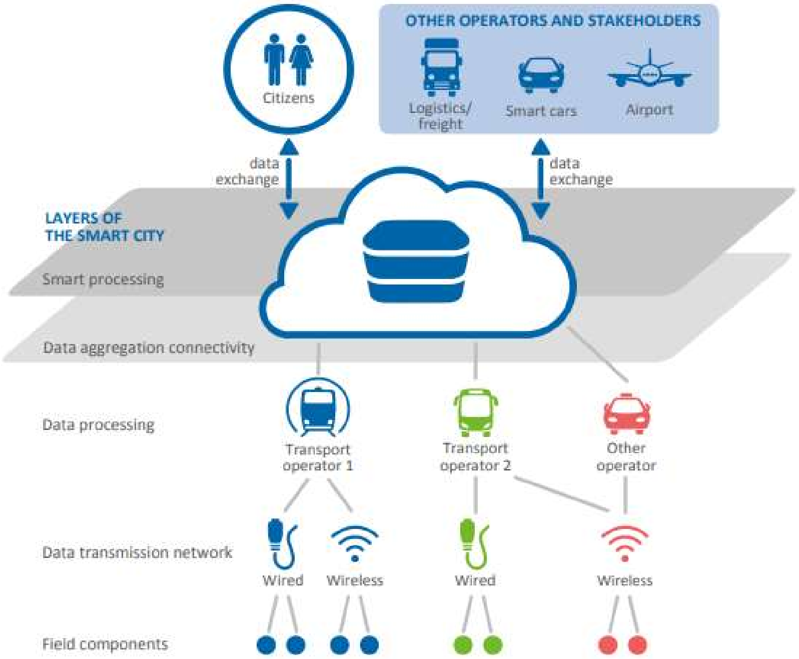
- The need for connectivity. Globalization and instant communication brought the desire for rapid connectivity. In this sense people started to work in other cities than the one that they are living, or generally, they started to travel more for different reasons. In order to make that possible, states or the local authorities needed to develop solutions, like for example fast trains that travel between various cities (the TGV from France).

- The desire for economic growth. Besides from the needs that are described above, the intelligent transport systems bring several benefits like: the reducing time for waiting, the interconnections that are possible in a faster way, the costs for transportation are lower, thus the city or the region would develop faster. Also we could take into consideration the indirect effects, like the attraction of foreign investors in a stable and sustainable environment, which in turn will create jobs and bring revenues to the local, regional budget.

In terms of objective and measurable benefits, according the some of the previous researches, we could identify the following:

- The increase of street throughput by 20–25% (Stawiarska and Sobczak, 2018, p.4) ;
- The traffic safety augmented, since the accidents number decreased by 40% until 80% (Stawiarska and Sobczak, 2018, p.4);
- Reduction of pollution;
- Economic development;
- The life quality of people increased since due to the fact that now people can learn about the seats available in a bus, the time remaining until the next bus arrives, the approximate time for reaching the desired location, the fast interconnections between trains, the push scooters available in their neighbourhood, etc.

All these are possible in a smart city that uses ITS, but in order to be able to provide these type of services, the ITS has to connect various actors like: users-citizens and stakeholders like public and private companies, different operating companies, etc., as it can be seen below:



Source: Cédric Lévy-Bencheton, Eleni Darra.2015. *Cyber security for Smart Cities An architecture model for public transport*. *Good practices and recommendations.* European Union Agency for Network and Information Security (ENISA).p.18

In terms of components, the ITS has to encompass the following: telecommunication technologies, information technology, methods of control and management of transport systems and networks and telematics of transport (Stawiarska and Sobczak, 2018, p.3). Besides these elements, every system needs a Traffic Management Centre that uses ICT systems, regardless of its specialization, namely traffic on land, on air, or on the sea. At the same time, in order for the Centre to work in an efficient way it needs to collect real time data regarding the traffic, the density of the population in a certain area in a certain period of time, real time accidents and alternative routes, etc. Additionally, after collecting the data, the Centre need to have transmission systems that send the collected data to the centre. Here timing is essential for the efficiency of the system. Last, but definitely not least, the centre needs to have operating systems and people that analyse the data very fast and adjust the system to meet the needs on the ground.

From a gamification perspective, all the elements that are present in the above image are linked through one or more application. Then, this app is used by the individuals for transport purposes. One classical app that is used all around the globe is Waze (2020). Through it the individuals can travel via car and on foot between different locations taking using live data regarding the traffic like traffic accident, traffic congestions, ways to avoid them, etc. The app is also designed to be friendly and to encourage competition since it offers rewards for those that are using it on regular basis. From the point of view of decision makers, the app is very useful since it offers essential information regarding the traffic at a specific hour, the preferred routes and the density of the population on a certain period of time and location, thus the tangible benefits for both individuals and the authorities. The app is also allowing the user to make reports or to communicate to other users regarding the traffic. This element is very important since the app is transforming the user in a part time operator, and like a living cell of the system it can influence it through its actions like for example reporting the presence of an accident or of the police where there is not the case. Waze proved to be successful since in August 2020 it has more than 90 million users (Waze and Drivers, 2020). Nevertheless, it has to be mentioned that gamification instruments are at the beginning stages of their development, therefore there are not very often found, thus their impact over the society is rather limited to different domains, like for example Waze in the case of land transportation.

At the same time, the app needs the location of the user and some of his/her personal data information like name, e-mail address, Facebook account. Here arises the issue of education, in the sense that the users should be aware of the requirements of the app and what they are entailing. From a security point of view, these opportunities can become a vulnerability if the necessary steps for protection are not in place as we are going to see in to following chapter.

Cyber-security of critical infrastructure within smart cities

At the level of the EU cyber-security is understood as "*collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*"(Lévy-Bencheton and Darra, 2015, p.14).

Returning to the architecture of a smart city, in terms of cyber-security we could identify the following issues. Taking into consideration all the layers and the actors that can influence the system's security willingly (hackers) or unwillingly (a user that is part of a botnet without knowing it or is hacked due to his/her security taken measures) or given the fact that the systems are interconnected, a hacker that gains access into the systems of transport *operator 1* and gain access or influence that data that transport *operator 2* is receiving. Thus, the range of possible cyber-attacks that can be inflicted against the systems pertaining to smart cities is very large. In this sense we could discuss about:

- Data stealing (number of persons that are connected and are using the subway in a specific moment during the day, their identify which in turn can be used later for fraudulent transitions);

-Hijacking of the system (the hacker can take control of the entire system which could cause even physical harm- e.g. the hacker can take control over the train, thus influencing the speed, the stops, and go even until the train will leave the tracks, therefore causing physical harm of the travellers, even death;

- Disturb and influence the information flow- e.g. the hacker can enter the system and make the Management Centre technicians and systems believe that the subway is going with a certain speed, when in reality the speed is much higher thus causing an accident;

- The classical DDoS in which the users cannot access the system to buy tickets anymore and last, but not least, blocking the system's operating tools until the municipality is paying the ransom;

- Breach of the confidentiality clause. An important element especially for the end users, the citizens, is represented by the protection of their data confidentiality (personal data like names, bank account number, etc.). Threatening this confidentiality would in turn break the trust of the citizens in the operators, be them public or private, which in turn would determine the user to choose other services or to mistrust the local, regional public institutions due to the loss of reputation;

- Trading information. Another possible threat is related to the available data, which can be exchanged between operators. Here, the EU is among the pioneers of the international system developing the GDPR through which it protects the data of its users.

Concrete examples of cyber-attacks that affected smart cities within the EU are the following:

1. November 2016, Sweden. Due to a cyber-attack the Air traffic controllers were not able to see the aircrafts on their screen. Due to the security issues that arose from this aspect and in

order to prevent accidents, numerous flights were cancelled, fact that affected a large number of individuals (IOActive, 2018, p.4).

2. October 2017, Sweden. The cyber-attack targeted the Transport Administration system through a DDoS. AS a result, the administrators had to operate the system manually, to stop some of the trains, facts that generated huge delays (IOActive, 2018, p.4).

Recommendations

In order to tackle all these vulnerabilities that decision makers should focus on public policies that provide the following services or implement the following activities:

- testing their critical infrastructure against possible cyber-attacks. In order to be able to protect themselves, their need to firstly establish their level of security. This will allow them to see which are the areas that need further investments in the security department.

- developing public-private partnerships between the local/regional governments and the private companies that operate the systems or private companies that are specialized in cyber-security aspects.

- creating Computer Emergency Response Teams (CERTs). This recommendation was already implemented as many countries in Europe already have such institutions: Netherlands, Romania, Belgium, France, Germany, Portugal, Luxembourg, Spain, Italy, Denmark, Sweden, Finland, Estonia, Lithuania, Latvia, Poland, the Czech Republic, Hungary, Slovenia, Croatia, Bulgaria, Greece, Austria, etc. (ENISA, 2020).

- developing cyber-attack emergency plans. Such plans would make possible the avoidance the replication of Estonia 2007 incident, or the ones from Sweden 2016 and 2017.

- making national awareness campaign to that to increase the knowledge level, thus the competences of the citizens regarding the online risks and ways to tackle them through cyber-hygiene or other means;

- making national awareness campaign to that to increase the knowledge level, thus the information of the citizens regarding the available application especially in the field of transportation;

- encouraging the private companies to disclosure the moments when they were victims of cyber-attacks. This recommendation is among the most difficult ones to implement, since by disclosing their security breaches the private companies can lose the trust of the costumers.

- training the security experts. An example in this case could be the Locked Shields exercise which take place in Estonia every year since 2010. "*For example, in the recent 2017 exercise, which involved nearly 900 participants from 25 nations, the teams were tasked to maintain the services and networks of a military air base of a fictional country, which, according to the exercise scenario, will experience severe attacks on its electric power grid system, unmanned aerial vehicles, military command and control systems, critical information infrastructure components and other operational infrastructure.*" (CCDCOE, 2019).

- integrating security standards at the EU level. For the harmonization of the security protocols and standards, the EU decision makers should agree on at least the minimum common denominator regarding the cyber-security requirements of smart cities.

- incorporating in the decision making process of the actors that are involved in the process (the public authorities, the private actors (manufactures, service providers, operators) and the end users).

- concentrating on the resilience of the system. Apart from protecting the system, the EU decision makers together with the national, regional and local ones should try to ensure the capacity of the system to recover in an acceptable timely manner, since in the cyber domain that question that should be posed in not if you get attacked, but when you do. Prevention is an important part of the strategy, but at the same time, given that fact that cyber threats and attacks do not have rather large costs to be deployed and the range of actors and their motives are heterogeneous the possibility of an attack is large, thus the security strategy should focus also on the steps that are to be taken after an attack happens.

- concerning strictly gamification, the decision makers should use more this technological instrument for cooperating or informing the population beyond the traditional channels. This could serve as a tools for increasing the transparency level, thus the trust of the population in the public authorities.

Conclusions

Nowadays society comes with unprecedented development. People can travel faster, safer at lower costs without affecting the environment. The initiative of smart city proved to be a very efficient one from both economic and environmental point of view. Coupled with the principles of gamification, the initiative created a network were the population is a directly involved actor that can influence the system. At the same time the technology comes with a cost and thus possible vulnerabilities in terms of security. From this point of view the article emphasized the possible threats for public authorities, economic operators and end users in terms of cyber-security within a smart city critical infrastructure framework. Referring to the specific case of the EU it must be said that besides that GDPR initiative that is meant to protect the ends users, it developed a specialized institution that is meant to tackle to issue of cyber-security at the level of the entire organization, ENISA. At the same time, we must not forget that the need for security is a pivotal responsibility of the national states, and apart from the classical meaning of the term, the XXI century poses new and very dynamic threats to which the states must adapt and respond.

Bibliography:

1. Buzan, B 1991, *People, states, and fear: an agenda for international security studies in the post-cold war era,* Boulder, UK.
2. Lévy-Bencheton, C, Darra, E 2015, *Cyber security for Smart Cities An architecture model for public transport. Good practices and recommendations*, European Union Agency for Network and Information Security (ENISA)
3. Zica MR, Ionica AC and Leba M 2018, "Gamification in the context of smart cities", in *IOP Conf. Series: Materials Science and Engineering 294, proceedings of the International Conference on Applied Sciences (ICAS2017),* viewed 30 July 2020, https://iopscience.iop.org/article/10.1088/1757-899X/294/1/012045/pdf
4. CCDCOE 2019, *Locked Shields*, viewed 25 August 2020, https://ccdcoe.org/exercises/locked-shields/
5. EUR-Lex 2009, *Council Directive 2008/11/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, https://eur-lex.europa.eu/legal-content/en/NIM/?uri=CELEX:32008L0114

6. ENISA 2010, *CERTs in Europe map,* viewed 30 August 2020, https://www.enisa.europa.eu/media/news-items/CERT_Euromap_2.0.jpg/image_view_fullscreen
7. EURACTIV 2020, "How many smart cities are there in Europe?", *EURACTIV*, August 2020, https://euractiv.eu/wp-content/uploads/sites/2/infographic/SMART-CITIES-20032017-EN-V02-A4-1.pdf , p.2-3
8. European Commission, Competence Centre on Foresight 2020, *Developments and Forecasts on Continuing Urbanisation European Commission,* viewed 14 August 2020, https://ec.europa.eu/knowledge4policy/foresight/topic/continuing-urbanisation/developments-and-forecasts-on-continuing-urbanisation_en
9. EUR-Lex 2020, *Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*, viewed 30 July 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040&from=EN
10. IOActive 2018, *Smart Cities Cyber Security Worries*, viewed 20 August 2020, https://ioactive.com/wp-content/uploads/2018/10/IOActive-SmartCities-cybersecurity-worries.pdf
11. EUR-Lex 2013, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0526*
12. 11. EUR-Lex 2019, REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Viewed 15 August 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG

13. Stawiarska, E and Sobczak, P 2018, “The Impact of Intelligent Transportation System Implementations on the Sustainable Growth of Passenger Transport in EU Regions” in *Sustainability*, 10, 1318
14. WAZE, https://www.waze.com, viewed 20 August 2020,