Efficient Workforce Management within the Concept of "Smart City". Using Artificial Intelligence as Part of the Future Counterterrorism Strategy

Mihai CONSTANTIN^{1*},
Anamaria BUCUR²
Andra-Nicoleta BORȚEA³

¹ Valahia' University of Targoviste,
Doctoral School, Targoviste, România,
constantintgv@gmail.com

² Valahia' University of Targoviste,
Doctoral School, Targoviste, România,
anamariabucur74@yahoo.com

³ Valahia' University of Targoviste,
Doctoral School, Targoviste, România,
andrabortea@gmail.com

* Corresponding Author

Abstract: Today, the world is going through an unprecedented wave of urbanization, an evolution that tends to focus on both the biggest social problems and the biggest opportunities in the area of big cities. Once the concept of "smart city" appeared brought its new challenges for our society. In addition to the many benefits, such as increased quality of life, a smart city is challenging the current government. The security of the citizens in the smart cities is gaining new perspective, but also brings a number of threats, mostly considering the strategies regarding counter-terrorism. The human component, specifically the workforce adapted to the smart city, faces new challenges: the emergence of artificial intelligence, increased demand for digital skills, a must have also in labour market, together with the technologization of all areas of activity, which produces changes in all aspects of daily life. Under these conditions, the human factor is affected by all these changes. One side of the story regards the training and, also, the education of individuals, which must increase digitalisation skills; the other side involves the government who must adapt its strategies and policies to enable these changes in a safe manner for citizens and public workers, who perpetuate these changes through local administrations. Therefore, human resources are an important component in the project that aims developing smart cities that includes also developing adapted protection for citizens, specific to these cities. The use of artificial intelligence in smart cities seems to be the solution to the problems raised by smart cities in relation to the human factor and its vulnerability. But at what cost?

Keywords: *artificial intelligence; security; smart city; public administration; fourth industrial revolution.*

How to cite: Constantin, M., Bucur, A., & Borțea, A.-N. (2020). Efficient Workforce Management within the Concept of "Smart City". Using Artificial Intelligence as Part of the Future Counterterrorism Strategy. In M. W. Staniewski, V. Vasile, & A. Grigorescu (vol. ed.), *Lumen Proceedings: Vol. 14. International Conference Innovative Business Management & Global Entrepreneurship (IBIMAGE 2020)* (pp. 715-725). Iasi, Romania: LUMEN Publishing House.
<https://doi.org/10.18662/lumproc/ibmage2020/52>

1. Introduction

In 1900, at the beginning of the second industrial revolution, with the advent of electricity and oil, only 200 million people lived in cities, or about one-eighth of the population [13].

A century later, starting with the early period of the “fourth industrial revolution”, which has as benchmarks artificial intelligence (AI), robotics, genomic editing and neurotechnology [21, pp. 23-24] people now live in smart cities and also operate here, surrounded by technology.

The United Nations forecasts indicate that the urban population will reach 5 billion by 2030 (60% of the population) [18].

For a sustainable development it is essential to manage this demographic change together with the socio-technological evolutions, especially for the conservation of the labour force, of the human resource, regarding the artificial intelligence.

Artificial intelligence, developed properly, offers endless opportunities in designing new facilities and services addressed to the inhabitants of the urban environment, but also makes possible the emergence of new vulnerabilities and risks that society must be prepared to manage effectively.

The aim of this paper is to project an overview regarding the period of fourth industrial revolution by the approach of the specificity of using artificial intelligence in the public sector, through an analysis of the benefits and risks resulting from technological development (including security risks arising from the use of technology by terrorist groups).

2. Problem Statement

The term smart cities, according to Harrison and Donnelly [12], has been used by global technology firms, especially since 2005 to “apply complex information systems to integrate the operation of urban infrastructure and services such as buildings, transport, electricity, water distribution and public safety” [16].

The term “smart city” has its origins in the 1990s and its appearance is due to IBM's effort to regain the previous level of profit, diminished in that period as a result of the recession [5]. Later, IBM disseminated and “sold” this expression to city representatives, who included it in the public discourse and made it known. In 2011, the term was officially attributed to IBM) [20].

Thus, IBM identified cities as a huge potential market to place services regarding information and communication technology [5].

Their concept had two postulates to start. First postulate refers to developing a city based on three pillars: service planning and management; infrastructure services; services offered by people.

The second postulate states that each of these pillars constitutes an individual system, the city transforming itself in a system made of systems [5].

It is important to note the presence of the human component and the services provided by people, even though the goal is digitalization of cities.

Origin and Definitions

Relying on urban marketing and advertising, the expression "smart city" is the phrase that could stand for the future version of a city, by emphasizing the change that new technologies will do in regards to urban spaces.

The definitions of the smart city, given in the literature, are numerous. Usually, the term "smart" is changed to "digital" or other similar terms. There is no template or model for framing smart cities or defining them [1].

One of the definitions of this mentions that the smart city is an area that creates sustainable development and high quality of life, par excellence in the fields of activity as a result of a solid human capital, social capital and ICT infrastructure, through the use of digital technologies to raise the standard of living, and by reducing costs and better communication with citizens. The smart city must be viewed from the perspective of its optimized functions and not through the amount of applications used [4].

A smart city has a wide range of eGovernment services and an infrastructure to implement the technology regarding information and communication, in order to generate public-private partnerships having as a goal to achieve the proposed objectives. It also needs eBusiness and eCommerce support to achieve these goals [4].

At the international level, the definitions of the smart city have different meanings.

The smart city concept is not limited to the frequent application of new technology in cities, but appeals to many sectors, which leads to some confusion between decision-makers at the urban level [2].

Another approach to this topic mentions that a city is smart when investments in human and social capital and in traditional (transport) and modern (ICT) communication infrastructure lead to sustainable economic growth and an increased quality of life [7].

The trend regarding urban population is the growth. This is why governments base their economic development policies on building advanced infrastructure to keep pace with development [3].

The definitions given by researchers tend to address three directions: smart cities in a vision that develop from smart technologies, smart cities from the perspective of the human resources, so called smart people and human success oriented towards the use and implementation of technology and smart cities with smart collaborations, i.e. with a government oriented towards the use and implementation technology [14].

All these approaches to different aspects of the concept show the tendency of researchers to explore only the desirable properties of a smart city. However, what would be really useful is a study that aims to develop a systematic understanding of city initiatives that turn them into smart or even smarter cities [1], but also, It would be more useful to develop a branch that combines the use of intelligent technology with the human component and artificial intelligence, without reducing the purpose of human in the labour market.

Therefore, technology remains the necessary basis for any smart city strategy [19].

3. Research Questions/Aims of the research

The research hypotheses of this paper are: The increased use of artificial intelligence in smart cities, instead of the classic human resources, attracts the risk of terrorist attacks upon the cities. This situation demands that the artificial intelligence must also be used in counter-terrorism strategies

4. Research Methods

In the process of validating these hypotheses, we used the empirical method of analysis of the literature and documents of public interest of specialized institutions, as well as the interpretation of data provided by specialized international platforms.

In the following paragraphs, we present the aspects of security in smart cities, from the perspective of digital evolution and technology both in public administration and labour market, but also regarding the security risks that comes as a package along with the increased technology level specific for digital revolution, mostly in mentioned fields.

5. Findings

The labour market in the smart city era. Trends and threats

Prototypes of artificial intelligence machines that succeed people are becoming more common. Although these robots will not take control of our lives very soon, there is a growing fear that they will soon replace us in our workplaces.

This option, in which the unskilled labour force would be successfully replaced by artificial intelligence raises many questions to the national governments, the most ardent being the salaries of the working people. A controversial solution is the existence of an income, seen as an universal base that ensures a minimum income for every citizen. The solution is imperfect and not just because it forces us to rely entirely on the government. Also, there is no unified decision on how to finance this, whether it is tax increases or other methods [15].

According to data provided by the European Commission, the number of jobs in the field of information and communication technology will increase by 16 million by 2020 [9].

Globally, there is an increasing demand for staff with digital skills. EU countries have a problem with a lack of ICT skills. The rapid development of technology has implications for "basic" jobs, which did not require any training or which required only basic training. They have undergone review processes on the skills required of the staff employed and the number of these jobs has been considerably reduced. Currently, citizens are subject to new, non-standard situations, for which they must develop new skills and knowledge [17].

At European level, it appears to be a need to invest in human resources, to educate them in order to adapt to the new information society, a society of digital cities, based on smart citizens, smart governance and smart technology.

In this regard, the European Union opens the subject of digital skills in the Digital Agenda for Europe, through a strategy that has as its ultimate goal both increasing productivity and increasing employment.

In 2017, more than half of EU companies that recruited or tried to recruit ICT specialists had difficulty filling ICT vacancies and 10% of EU companies provided their ICT specialists with vocational training, while twice as many have provided ICT training for others [10]. It can be concluded that companies in the ICT sector employ and recruit more ICT specialists than other sectors.

In 2018, one in five EU companies hired ICT specialists (20%), with the highest proportion observed among companies in the information and

communications sector (74%). Overall, this sector accounts for almost 4% of EU businesses with at least 10 people employed. For other sectors, the percentage of enterprises employing ICT specialists ranged from 8% in construction to 31% in professional, scientific and technical activities [10].

In Conclusions on the Future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion", 2019, the Council of the European Union highlights that digital development, including the development of digital skills (e.g. digital skills needed for and industrial services, cybersecurity and emerging key technologies (such as artificial intelligence and high-performance computing), for the benefit of all, must be provided, thus preventing digital sharing and creating the conditions for a more inclusive digital economy. Education, training, social protection of new forms of work, including for vulnerable groups, as well as the social rights of workers must be central concerns, best adopted in a national lifelong learning strategy [11].

The lack of digital skills has many negative consequences for the digital society. This lack can lead to an increase in the long-term unemployment rate, as these skills condition the return of a person in a search of a job, back to labour market. The lack of digital skills also leads to a slowdown in the digitalisation of cities, as well as an increased risk of not being able to cope with terrorist cyber-attacks, especially in smart cities or those in the process of becoming smart.

6. Conclusions

The Security in the Smart City

Today, urban services need a transformation, and not only the public services, but the public administration and the entire system. The transformation can take place through the implementation of 5G technology or Internet of Things, aiming to improve the citizen-local administration interaction [8].

However, following the transformation of urban services, smart or even smarter cities can become targets for cyber actors. They can exploit vulnerabilities in digital security systems to affect or stop the services provided. Therefore, the evolution of technology implies an evolution of cyber security. The technology we use today has a growing impact on physical space, increasingly exceeding digital boundaries. This fact requires us to understand the risks of a weak digital security to which we are exposed, both as individuals and at the organizational level [8]. As AI capabilities increase, we expect major changes in the type of security threat and new implications that will result from the materialization of those threats.

We can predict an increase in existing threats due to the use of AI systems to perform tasks that would normally require human involvement, information and high expertise.

At the same time, we will see an increase in the following components: the number / categories of people who can carry out attacks (because the implementation with technology will be easy), the speed with which the attack will occur (important aspect for possible counteraction) and the set of possible targets.

New threats will arise. In the future, the use of technology will make it possible to carry out attacks that, at present, cannot be carried out by human intervention (eg the use of a harmful nuclear, chemical or biological environment, access to isolated or difficult-to-penetrate environments).

The typology of threats will change. Attacks made with AI will be particularly effective, very well targeted and difficult to assign.

We can divide the concept of "Security" Smart city into three [6] constituent parts, which make up the picture of new threats:

1.Digital security - on the first component, the aim must be to ensure the optimal level of security of the cyber infrastructure (which due to the implemented technologies plays a major role in Smart City). From this point of view, we can say that security assurance is a collaborative project involving many partners - sensor manufacturers, gateway providers, standardization bodies, security software, developers of operating systems specializing in infrastructure and of course, public authorities. All these actors are an essential part of a complete, vital and connected IoT (acronym for Internet of Things) security ecosystem.

The effort to secure smart cities can be achieved through three major actions:

Table 1. Actions to secure smart cities

Choosing the right technologies	At the heart of the infrastructure, technologies must natively integrate the concepts of security (secure authentication, usage controls, etc.) and confidentiality, while allowing interoperability with the other elements of the chain. These technologies also need to be updated regularly.
Performing security tests	As with large IT firms, which regularly simulate intrusions into their systems, Smart City infrastructures must be tested regularly for possible security breaches.

	These tests are an opportunity to configure processes that can be triggered in the event of an intrusion.
Domain organization:	Security officials need to increase their level of agility and adaptability in order to have a cross-sectional view of the projects they work on.

Source: Brundage et al. 2018 [6]

At the same time, the use of malicious Artificial Intelligence, by automating parts of a cyberattack, will increase the effectiveness of attacks. There are planned new types of attacks, that will target the exploitation of human vulnerabilities, software (e.g. automatic hacking) or AI systems (e.g. providing conflicting data to AI systems).

2. Physical security - Use of Artificial Intelligence to carry out complex attacks with autonomous components (e.g. drone attacks or autonomous firearm attacks). Incidents with major security implications can be made by hijacking autonomous cars and directing them to crowded areas or simply taking control of remote-controlled aircraft and crashing them.

3. Political security - The use of artificial intelligence for the implementation of population surveillance systems (e.g. collection and analysis of personal data), persuasion (e.g. propaganda / counter-propaganda operations) and deception (e.g. falsification of videos and using them as “fake news”). New technologies can be used for complex invasive processes of privacy and social manipulation. At the same time, the malicious use of technology, of new processes that will allow the automatic analysis of human behavior, mood, etc., can be exploited by authoritarian states, in order to undermine democratic elements.

Defensive use of artificial intelligence

The same features of artificial intelligence that allow attacks to be carried out in a broad way and with minimal costs, make it possible to develop a new defensive strategy, applicable to the three security niches described above.

Regarding digital security as a countermeasure to the new categories of attacks, we expect the creation of spam filters and effective malware detection systems. In the area of physical security, we expect the defensive use of drones to capture / neutralize drones used in attacks or monitor with these devices some areas at risk. These defensive actions will be necessary and will be carried out on a large scale. For a full analysis of the concept with

the purpose of using technology regarding the security area, we should consider also the costs involved, that need to be taken into account.

A broad area in which the use of artificial intelligence can be used is the field of anti-terrorism / counter-terrorism.

The use of facial recognition technology or monitoring of social networks to identify possible people with concerns that contravene the law, will be able to allow early intervention, through rapid detection and effective response.

References

- [1] Alawadhi S, Aldama-Nalda A, Chourabi H, Gil-Garcia JR, Leung S, Mellouli S et al. Building understanding of smart city initiatives. In Electronic Government - 11th IFIP WG 8.5 International Conference, EGOV 2012, Proceedings. 2012. p. 40-53. (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)). Available from: https://doi.org/10.1007/978-3-642-33489-4_4
- [2] Albino V. Berardi U. Dangelico RM. Smart cities: Definitions, dimensions, performance, and initiatives. Journal of Urban Technology [Internet]. 2015 [cited 2020 August 18]; 22(1); 3-21. Available from: <https://doi.org/10.1080/10630732.2014.942092>
- [3] Bakici T. Almirall E. Wareham JA. Smart City Initiative: The Case of Barcelona. Journal of the Knowledge Economy[Internet]. 2012[cited 2020 August 18]; 4(2):135–148. Available from: <https://doi.org/10.1007/s13132-012-0084-9>
- [4] Baltac V. The Smart City and the Digital Gap. In Dinca D, Vrabie C, Dumitrica C, editors. The “Smart City” Scientific Communications Session, Third Edition [Internet]. Bucuresti: Pro Universitaria; 2016. [cited 2020 August 11]. p. 12-13. Available from: https://www.researchgate.net/profile/Catalin_Vrabie/publication/309203970_Sesiunea_de_comunicari stiintifice Orasul inteligent Smart Cities Proceedings_vol_3/links/58051ec808aee314f68e20a6/Sesiunea-de-comunicari-stiintifice-Orasul-inteligent-Smart-Cities-Proceedings-vol-3.pdf
- [5] Breux S. Diaz J. The smart city. Origin, definitions, strengths and limits of a polysemic expression. Montréal: Institut national de la recherche scientifique Centre - Urbanisation Culture Société. 2017 Janvier [cited 2020 April 29]. 31 pages. Available from: <http://espace.inrs.ca/id/eprint/4917/1/Rapport-LaVilleIntelligente.pdf>
- [6] Brundage M. Avin S. Clark J. Toner H. Eckersley P. Garfinkel B. Dafoe A. Scharre P. Zeitzoff T. Filar B. Anderson H. Roff H. Allen G. C. Steinhardt J. Flynn C. HÉigeartaigh, S. O. Beard S. Belfield H. Farquhar S. Lyle C. Crotoof

- R. Evans O. Page M. Bryson J. Yampolskiy R. Amodei D. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation [Internet]. Oxford: University of Oxford; 2018 February [cited 2020 July 28]. 101 pages. Available from: https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf
- [7] Caragliu A. Del Bo C. Nijkamp P. Smart Cities in Europe. Journal of Urban Technology [Internet]. 2011 [cited 2020 August 18]; 18(2):65–82. Available from: <https://doi.org/10.1080/10630732.2011.601117>
- [8] Căzăceanu E. Virtual projection in the real world. Intelligence Magazine [Internet]. 2020 May 12 [cited 2020 August 18]. Available from: <https://intelligence.sri.ro/proiectii-virtuale-lumea-reala/>
- [9] European Commission. Understanding European Union Policies. The Digital Agenda for Europe. Brussels: European Commission. 2014 November [cited 2020 August 18]. p. 3. Available from: file:///C:/Users/user/AppData/Local/Temp/gp_eudor_WEB_NA0114996ENC_002.pdf.en.pdf
- [10] European Commission. Eurostat 2018, ICT specialists - statistics on hard-to-fill vacancies in enterprises [Internet]. 2018 [cited 2020 August 18]. Available from: https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises#Employment_and_recruitment_of_ICT_specialists
- [11] General Secretariat of the Council, Council of the European Union, [Internet]. 2019, June [cited 2020 July 27]. Conclusions on the Future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion", Council of the European Union. Available from: <https://www.consilium.europa.eu/media/39667/st10102-en19.pdf>
- [12] Harrison C, Donnelly IA. A Theory of Smart Cities. ISSS-2010 [Internet]. 2011 Sep. 23 [cited 2020 Oct. 30]; 55(1). Available from: <https://journals.iss.org/index.php/proceedings55th/article/view/1703>
- [13] Malcolm F. Roehrig P. Pring B. What To Do When Machines Do Everything: How to Get Ahead in a World of AI, Algorithms, Bots, and Big Data. United States Of America: Wiley. 2017 February 13, p. 14 [cited 2020 April 29]. 256 p.
- [14] Meijer A. Bolívar MPR. (2015). Governing the smart city: a review of the literature on smart urban governance. International Review of Administrative Sciences [Internet]. 2015 [cited 2020 August 18]; 82(2):392-408. Available from: <https://doi.org/10.1177/0020852314564308>
- [15] Moeller M. Automation Is on Its Way, Can Blockchain Help Save the Workforce. Be[in]crypto [Internet]. 2019 July 2 [cited 2020 July 27]. Available from: <https://beincrypto.com/automation-is-on-its-way-can-blockchain-help-save-the-workforce/>

- [16] Paroutis S, Bennett M. Heracleous L. A Strategic View on Smart City echnology: The Case of IBM Smarter Cities during a Recession. Technological Forecasting and Social Change. Special issue Upgrading a City via Technology [Internet]. 2014, November [cited 2020 July 27]; 89: 262-272. Available from: <http://dx.doi.org/10.1016/j.techfore.2013.08.041>
- [17] Petre I. Cristescu I. The citizen and the challenges of the information society. Romanian Journal of Information Technology and Automatic Control [Internet]. 2019 [cited 2020 July 27]; 29(1): 59-68. Available from: <https://doi.org/10.33436/v29i1y201906>
- [18] Pitroda S. Mialhe N. Introduction. The rise of AI and robotics in cities. Field Action Science Reports [Internet]. 2017 [cited 2020 April 29]; 17. Available from: <https://www.institut.veolia.org/fr/our-contents/veolia-institute-review-facts-reports/intelligence-artificielle-et-robotique-dans-la>
- [19] Sajhau P. IBM – Building sustainable cities through partnerships and integrated approaches. Field Actions Science Reports [Internet]. 2017 June 01 [cited 2020 April 29]; Special Issue 16. Available from: <http://journals.openedition.org/factsreports/4345>
- [20] Söderström O. Paasche T. Klauser F. Smart cities as corporate storytelling. City: analysis of urban trends, culture, theory, policy, action [Internet]. 2014[cited 2020 April 29]; 18(3): 307-320. Available from: <https://doi.org/10.1080/13604813.2014.90671>
- [21] Toffler A. Toffler H. War and anti-war. New York: Warner Books. 1995.