THE EFFECTS OF GLOBALIZATION AND CYBER SECURITY ON SMART CITIES

Zsolt Szabó*

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.17.3.10
Regular article

Received: 7 December 2018.
Accepted: 31 August 2019.

ABSTRACT

By 2050, 70% of all people will be living in towns and cities. In 1900, it was only 13%. This means that every year, the number of people living in cities increases by seven times the population of New York. Water usage is increasing rapidly too; it has sextupled in the past 100 years; this rate of increase is double the rate of population increase. We must all face the challenge of a large number of people living together efficiently, in an organized way, on Earth, and how they can all access the needed services with the required quality. The term smart city primarily emphasizes sustainability, efficiency, and wide participation in decision-making, infocommunication technology solutions and providing services. The term was coined based on the integration of digital technologies, and the important phenomenon of community development and economic innovation, cities. The main players in the economy of the future are cities. States and local governments alone cannot respond to the challenges of global urbanization and environmental issues. In the development of smart cities, players of the economy and the city dwellers themselves play a more and more important role. The European Union has started programs like this and it is of paramount importance that Hungary actively participates in these, both in central coordination and at the level of settlements. At the same time, it is great help for Hungarian enterprises, too because the products they develop in and for Hungarian towns can be competitive on the international market as well.

KEYWORDS

smart city, cybersecurity, information security, IT security, threats and risks

CLASSIFICATION

JEL: F50, F61, H12, I23, J28

*Corresponding author, η: szabo.zsoltmihaly@phd.uni-obuda.hu; +361 666 5375;
DSSSS, Óbuda University, Bécsi út 96/b., H-1034 Budapest, Hungary

GLOBALIZATION AND INFORMATION SECURITY

Our world suffers three great impacts at the beginning of the 21st century: the population explosion, the increase in life expectancy and the information explosion [1]. The "demographic time bomb" or "population bomb" (the problem of aging) will affect the whole world socially, economically and in other ways. The UN declared 11 July World Population Day in 1989 because the population of the world surpassed 5 billion exactly 2 years before. Since then, world population has increased by more than 2.6 billion, and on 1 July 2018, it surpassed 7.6 billion. World population in 1950 (2.5 billion) has more than tripled by now. Population is still increasing although at a decreasing rate. The United Nations Department of Economic and Social Affairs (DESA) forecasts (assuming medium level fertility) [2] that world population will reach 10 billion by 2055, and by 2100, 11.2 billion people will live on Earth. In 1950, less than 30% of the population lived in cities. In 2018, however, 55% people were city dwellers. The trend is predicted to continue and it is forecasted that in 2050, 68% of people will live in cities. According to the demographic data of the UN (Fig. 1) the population of the world is increasing because the population of developing countries (where many people are very poor) is increasing fast. The population of developed, industrialized countries is decreasing.

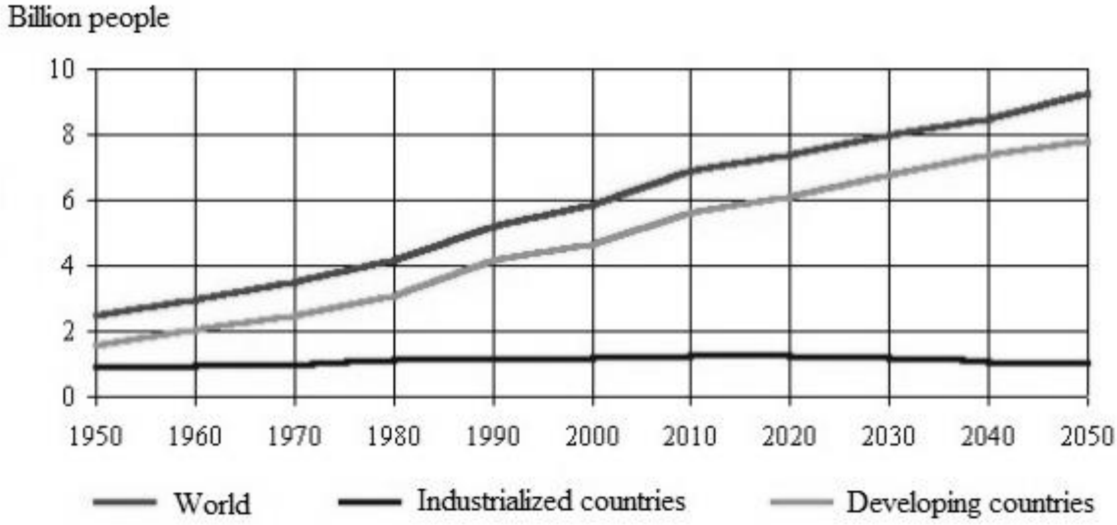


Figure 1. World population between 1950 and 2050.

The UN has been making estimates since 1988 concerning the distribution of the population within countries, and the number of people living in villages, towns and cities. In May 2018, they published the predictions for urbanization until 2050, which was based on the previously mentioned UN population forecast of 2017 [3].

Information concerning the urbanization processes of the world is indispensible for the setting of community development goals both in cities and in the country. The ratio of urban population is considered a basic indicator of economic and social development. For this reason, the increase of urbanization in space and time indicates development well. Urbanization can be charactierized by the increase in the number of cities and the number of people living in the cities. In 1950, less than 30% of people lived in cities. In 2010, the number of people living in cities reached the number of people living in the country. In 2018, 55% of people lived in cities. The number of city dwellers in the world has increased 5,6 times (to 4,2 billion) since 1950 (751 million), while the number of people living in the country has only doubled since 1950 (to 3.4 billion) (Fig. 2). This tendency is forecasted to continue—in 2050, 68% of people will live in cities [3].

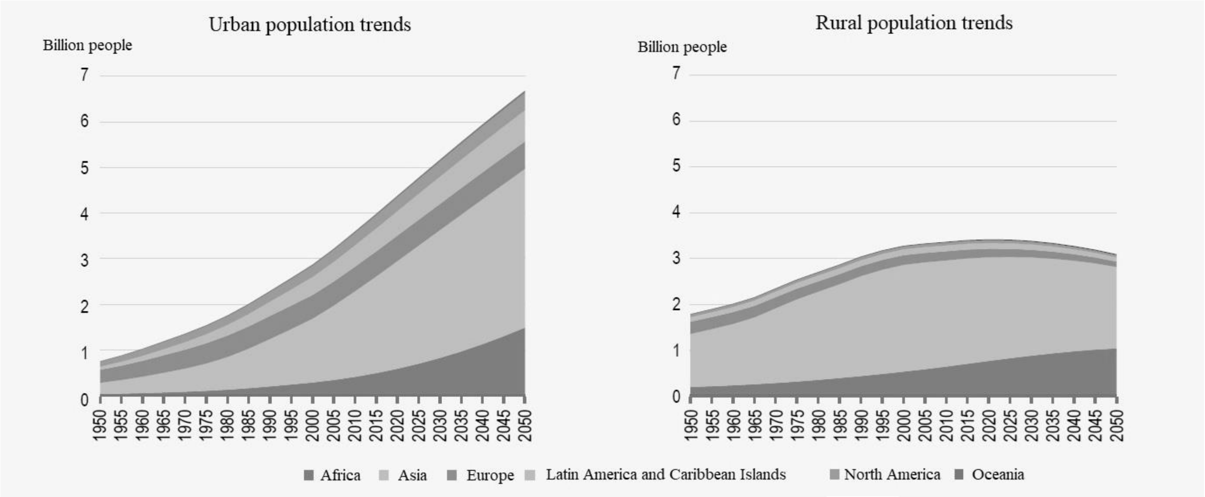


Figure 2. Population in cities and in the country between 1950 and 2050.

Forecasts show that urbanization and the general increase in world population will result in the number of city dwellers increasing by 2,5 billion by 2050. Nearly 90% of this will concentrate in Asia and Africa. It can be seen that by 2050, nearly 70% of people will live in cities. Urbanization is a dual process; on the one hand it means the increase in the number of cities, while on the other hand it means the expansion of urban functions, the development of infrastructure and city lifestyle.

One of the main tools and also channels of globalization since the 1990s is the explosive development of the Internet and mobile telecommunication technologies. As computers developed, after a time, the Internet was created [4, 5].

Web 1.0 covers the period between 1989 and 2004-2005. It is also referred to as the era of information connections. In other words, this was called "read-only web" [6]. In the early days of the Internet, you could search for and read information on the Internet. Very little interaction was offered to users, connection to websites was nearly impossible, and content production was practically non-existent. Website operators did not want to communicate with the visitors of the website, just provide them with information, anybody, any time. Therefore, at the dawn of the Internet, it was very static, "read-only", and with very little content produced. Each website had a limited number of people responsible for it. The websites could not be edited by anyone, just people who had permission to do it and access. It was their responsibility to keep the site up-to-date and to transmit the fresh content to the users.

The second generation of the Internet, Web 2.0, defined as "readable and writable web" [6]. Over the years it had very many definitions. Web 2.0 is a revolution in the commercial world of the IT industry, used as a platform. The basic difference between Web 1.0 and Web 2.0 is that there were few content producers with the first generation. Most Internet users behaved like people in a shop. They browsed the selection but did not add anything to it. On the other hand, in the era of Web 2.0, anybody can be both a seller and a buyer at the same time. Many technological solutions have been created to help users create their own content, and thus facilitate the mass production of content.

Web 2.0 is an umbrella term, including a multitude of Internet services. All such services are based on the power of the community. Users create content together or share each other's information [7]. The democratic nature of Web 2.0 is shown by a large number of Niche groups (closed communities of friends), who can exchange, label, comment or link an content, be it text, sound, images or video, to sites within or outside the group. Web 2.0 was the basis of the first social media sites, too. It is hard to imagine the world, when social media sites were not part of our everyday lives. By now, the Internet has become a utility. Not a day passes by when we do not look up on the Internet what has happened in the world. We no longer get the most news from newspapers, the radio or television, but read news on the Internet or listen to it on net radio. Today’s households require service providers to develop; this can be seen in every service sector. Whatever we plan to buy, we first look it up on the Internet, read about its properties and read opinions and other people’s experiences and only then decide to buy it. We select the best or cheapest shop on the Internet and buy the product or service there.

As opposed to Web 1.0 and Web 2.0, Web 3.0 is no longer made for people only, and not only people will use it. Nowadays the Internet can be accessed from nearly everywhere in the world [7]. Now global IP traffic has exceeded one zettabyte (10^{21} byte). Only in Google, 3 600 000 searches are executed every minute, and in one year, four billion people will have Internet access. Facebook had more than 2 billion active users in 2017. Web 3.0 is an exceedingly tailored web, which is decentralized and provides users with more possibilities than ever before. As a result of the population explosion and information explosion, we must all face the challenges of the global digital world; the most important challenge is how all these people can live together efficiently, in an organized way, and how they can access the right type of digital and other services in the right quality and with the required security. Another challenge is to train enough specialists who can design, install and operate the necessary systems.

CYBERSECURITY ISSUES IN A SMART CITY

Currently there is no universally accepted definition for cyberspace. The term Cyberspace (cybernetics + space) was coined by William Gibson science fiction writer in 1982. It first appeared in his short story “Burning Chrome” [8], then in his 1984 novel Neuromancer [9]. Over the years there have been countless definitions for cyberspace [10, 11]. Based on these, in general, cyberscpace can be considered a system of electronic communication devices and systems (computer networks, telephone lines, satellite systems etc.) and the virtual space composed of the services provided on these. As the Internet is growing and spreading, more and more formerly independent communication networks, systems, devices and services are connected to it, or simply being replaced by the Internet. Therefore, it is not surprising that in everyday use, the concept of cyberspace is more and more understood as the Internet itself, or the virtual world accessible through the Internet. The technological revolution mentioned earlier and cyberspace are changing our everyday environment more and more intensively, from communication, through access to services, to the data available to decision makers.

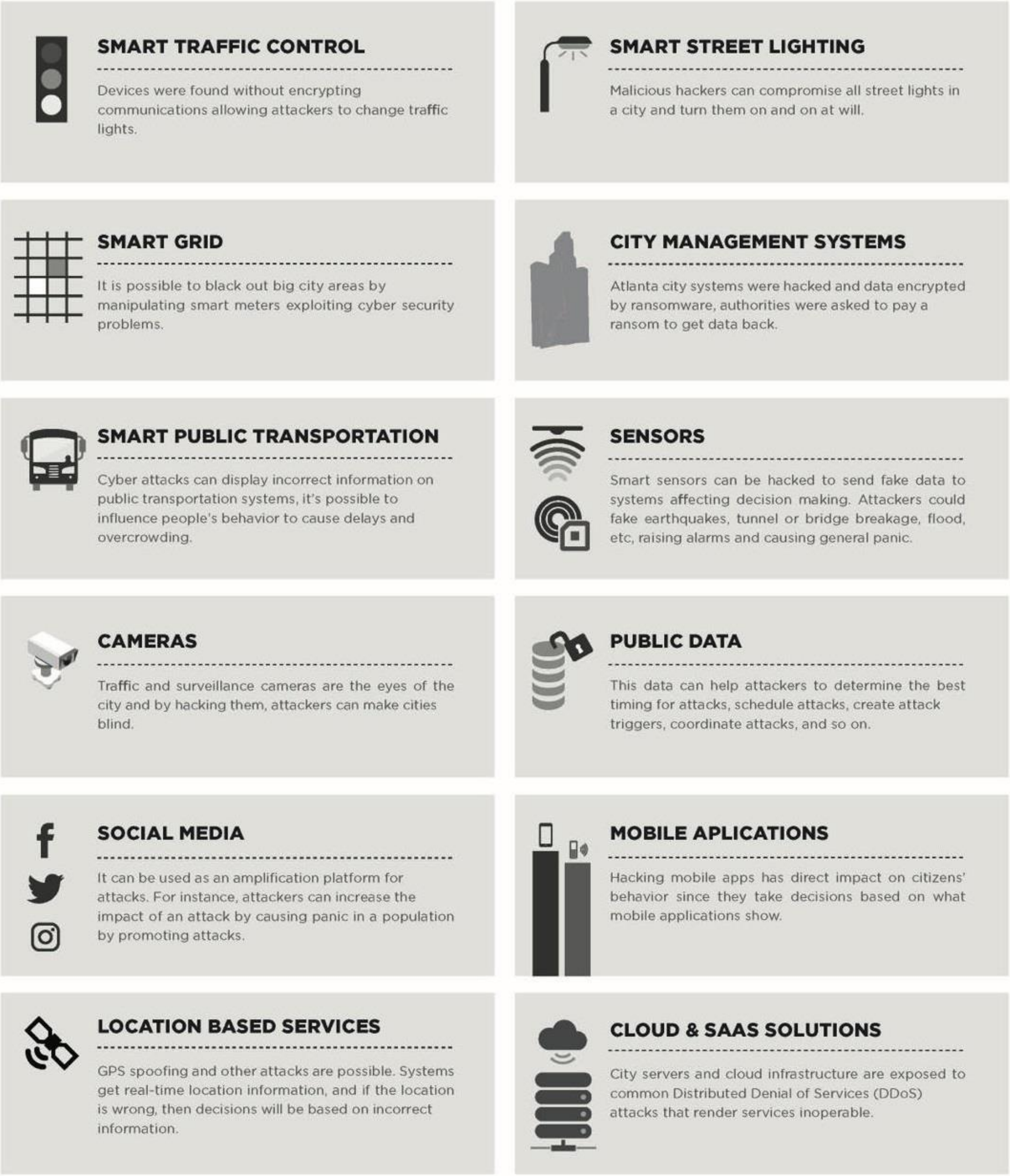
The term “Smart City” was invented in the USA. A city can be called smart if it achieves sustainable economic development with balanced investment in traditional and digital infrastructure, and human and social capital, with the active participation of the community, in an environmentally conscious way [12].

For a city, being a smart city is a process; it involves continuous development. Intelligent cities consist of many different and connected components, which continuously exchange data. Components can be intelligent networks, building automation systems, intelligent vehicles (driverless or pilotless vehicles, and others), Intenet of Things (IoT) sensors and using the cloud platform [13].

CYBERATTACKS AND THREATS

Smart cities process an enormous amount of data, due to the smart devices. These devices collect and generate many different kinds of information (sensor data, location data, common routes, and even customs of the citizens). Processed properly, these data provide valuable information in many areas [14, 15]. Internet-enabled devices, for example, can diagnose themselves, and so the can predict maintenance needs or even future breakdowns. Examining user customs can also help manufacturers to develop more convenient and safer devices. Another possibility is that manufacturers can pass on or sell aggregated anonymous data to other organizations, this way helping design and maintenance. This, however, is both a possibility and a danger (Figure 3) [16, 17].

Smart cities are comprised of a highly complex, interdependent network of devices, systems, platforms, and users. Smart energy, utilities, water and wastage, parking and automotive, industrial and manufacturing, building automation, e-government and telemedicine, surveillance and public safety are just some of the verticals that vendors and governments must secure. Urban population is on the rise worldwide and smart city development projects are



SMART TRAFFIC CONTROL

Devices were found without encrypting communications allowing attackers to change traffic lights.

SMART STREET LIGHTING

Malicious hackers can compromise all street lights in a city and turn them on and on at will.

SMART GRID

It is possible to black out big city areas by manipulating smart meters exploiting cyber security problems.

CITY MANAGEMENT SYSTEMS

Atlanta city systems were hacked and data encrypted by ransomware, authorities were asked to pay a ransom to get data back.

SMART PUBLIC TRANSPORTATION

Cyber attacks can display incorrect information on public transportation systems, it's possible to influence people's behavior to cause delays and overcrowding.

SENSORS

Smart sensors can be hacked to send fake data to systems affecting decision making. Attackers could fake earthquakes, tunnel or bridge breakage, flood, etc, raising alarms and causing general panic.

CAMERAS

Traffic and surveillance cameras are the eyes of the city and by hacking them, attackers can make cities blind.

PUBLIC DATA

This data can help attackers to determine the best timing for attacks, schedule attacks, create attack triggers, coordinate attacks, and so on.

SOCIAL MEDIA

It can be used as an amplification platform for attacks. For instance, attackers can increase the impact of an attack by causing panic in a population by promoting attacks.

MOBILE APLICATIONS

Hacking mobile apps has direct impact on citizens' behavior since they take decisions based on what mobile applications show.

LOCATION BASED SERVICES

GPS spoofing and other attacks are possible. Systems get real-time location information, and if the location is wrong, then decisions will be based on incorrect information.

CLOUD & SAAS SOLUTIONS

City servers and cloud infrastructure are exposed to common Distributed Denial of Services (DDoS) attacks that render services inoperable.

Figure 3. The challenge of securing smart cities: cyberattacks and threats.

are harnessing the power of the Internet of Things (IoT) to develop more intelligent, efficient, and sustainable solutions [18]. However, digital security investments in smart cities are severely lagging thus seeding the future vulnerabilities of the IoT ecosystem. Cyber attacks targeting IoT devices are rapidly increasing, as more people and organizations deploy them. IoT devices that are connected to the Internet but do not have a password set, or are often operated with the initial settings, are likely candidates to be targeted next. The security measures covering IoT devices are urgently needed [19].

IoT devices, which have smart functions and are connected to the Internet are among the most important and fastest growing segment of technology. The value of IoT is estimated to reach 83 billion dollars by 2022. The security of all the data used by IoT is a serious challenge. According to recent statistics, attacks against the IoT have increased sixfold between 2014 and 2018. These incidents affect all players of the sector, from manufacturers and their suppliers to operators. manufacturers have to protect more and more data. A device connected to the Internet may process several Gigabytes of data in a single hour. In the third quarter of 2018, only in the USA, on the telecommunications network of AT&T, 24 million connected devices communicated with each other. If these data are stolen or made public, it can lead to serious damage, and hefty fines in this better and better regulated environment. IT experts therefore have to guarantee not only the fast and efficient use of data but also their secure handling, according to GDPR [20] and other laws and regulations. Experts say that an obvious solution of protecting sensitive data is removing the sensitive parts from data before they enter analytical platforms. One method to do this is data masking, which involve changing sensitive data to random characters. Its advantage is that the format of the data remains and therefore the data can be used in various analyses and statistics.

CYBER PROTECTION AND CYBER STRATEGIES

As infocommunication devices and services develop rapidly, more and more cyberattacks are directed towards the state, civilian and private sector [21, 22]. In the past few years, several international organizations have offered recommendations, strategies and norm frameworks so that states and social and economic players can develop their own cyber protection structure and generate the minimum requirements that are essential safe and secure existence in cyberspace. The NATO cyber protection centre (2010) [23]; the International Telecommunication Union of the UN (2017, 2018) [22, 23], the European Union Agency for Network and Information Security (ENISA) (2017, 2018) [26, 27], Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [28]. These all call our attention to basic and interconnecting security situations:

- any member of information and communication networks – whether international, state or civilian – can be a potential victim of cyberattacks,
- cyberattacks can have serious national security and economic consequences, and can endanger the everyday life of a society,
- defence agains threats is a task at the international, national and individual user level as well.

CONCLUSION

At the beginning of the 21st century world economy was far more integrated than in the middle of the 20th century. It is visible that there are three large centres in world economy: North America, Western Europe and Eastern Asia. China is the most populous country in the world and the largest aging society. The problem of aging societies affect the whole world in one way or another. The main factors of economy in the future will be cities. “Smart city” is not a state, rather a process, the result of continuous development. The smart city concept, however, is a serious security risk all over the world, due to the infocommunication and other systems, which are not always secure. The first – and perhaps most serious – security issue is dependence. Dependence on infocommunication systems and the services they provide. When smart services falter in a city space, which is overcrowded in itself, and whose efficient operation heavily relies on information systems, enormous chaos ensues. From transport through logistics to public utilities, all systems are more and more interdependent. In this situation, a carefully planned and executed IT or information attack can easily bring a city to its knees. There will be no disposal of waste, passanger transport falters, there is no transport of goods, no communication; there is not even news about what happened. Of course, this is only fiction now, and smart cities have no alternative. Therefore security and secure systems are the only alternative for the future.

REFERENCES

[1] Iván, L.: *Physiological and social phenomena of aging. Current issues of aging.*
Journal of the Hungarian Academy of Sciences **2002**(4), 412-418, 2002,

[2] United Nations (DESA): *The 2017 Revision of World Urbanization Prospects.*
https://esa.un.org/unpd/wup, accessed 13th May 2019,

[3] United Nations (DESA): *The 2018 Revision of World Urbanization Prospects*.
https://esa.un.org/unpd/wup, accessed 14thMay 2019,

[4] *Internet History of 1990s.*
https://www.computerhistory.org/internethistory/1990s, accessed 15th May 2019,

[5] –: "*World Wide Web Timeline".*
Pews Research Center,

[6] Viswanathan, G.; Mathur, D.P. and Pradeep, Y.: *From Web 1.0 to Web 2.0 and beyond: Reviewing usability heuristic criteria taking music sites as case studies*.
https://www.academia.edu/8381037/From_Web_1.0_to_Web_2.0_and_beyond_Reviewing_usability_heuristic_criteria_taking_music_sites_as_case_studies, accessed 18th May 2019,

[7] Cohen, B.: *Urban Mobility: Web 2.0 (Uber) vs. Web 3.0 (IoMob).*
https://medium.com/iomob/urban-mobility-web-2-0-uber-vs-web-3-0-iomob-2e424a99f8bd, accessed 20th May 2019,

[8] Gibson, W.: *Burning Chrome. Burning Chrome.*
HarperCollins Publishers Inc., New York, 1986,

[9] Gibson, W.: *Neuromancer*. 20th Anniversary Edition.
Ace Books, New York, 2004,

[10] Haig, Zs.: *Information, Society, Security*.
NKE Service Ltd., Budapest, 2015,

[11] Gémes, Cs.: T*he cyberspace and its actors.*
Hadmérnök **13**(3), 403-415, 2018,

[12] Giffinger, R.: *Smart cities Ranking of European medium-sized cities.*
http://www.smart-cities.eu/download/smart_cities_final_report.pdf, accessed 23rd May 2019,

[13] Tokody, D.; Albini, A.; Ady, L.; Rajnai, Z. and Pongrácz, F.: *Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city*.
Interdisciplinary Description of Complex Systems **16**(3-A), 384-396, 2018,
http://dx.doi.org/10.7906/indecs.16.3.11,

[14] Szabó, Zs.*: Cybersecurity issues of pension payments.*
In: IEEE 15th International Symposium on Intelligent Systems and Informatics. IEEE, Subotica, 2017,
http://dx.doi.org/10.1109/SISY.2017.8080569,

[15] Szabó, Zs.: *Cybersecurity issues in industrial control systems.*
In: IEEE 16th International Symposium on Intelligent Systems and Informatics. IEEE, Subotica, 2018,

[16] Swati, K.: *TheHackerNews: Baltimore City Shuts Down Most of Its Servers After Ransomware Attack.*
https://thehackernews.com/2019/05/baltimore-ransomware-cyberattack.html, accessed 25th May 2019,

[17] Gibbs, S.: *Ransomware attack on San Francisco public transit gives everyone a free ride*.
https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware, accessed 26th May 2019,

[18] Help Net Security: *Cybersecurity challenges for smart cities: Key issues and top threats*.
https://www.helpnetsecurity.com/2019/08/21/cybersecurity-smart-cities, accessed 21st August 2019,

[19] Abdulmalik, H.; Jingqiang, L.; Fengjun L. and Bo, L.: *Cyber-Physical Systems Security – A Survey*.
IEEE Internet of Things Journal **4(**6), 1802-1831, 2017,
http://dx.doi.org/10.1109/JIOT.2017.2703172,

[20] –: *Regulation (eu) 2016/679 of the european parliament and of the council.*
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, accessed 26th May 2019,

[21] Pető, R.: *Security of smart city*.
Interdisciplinary Description of Complex Systems **17**(1-A), 13-19, 2019,
http://dx.doi.org/10.7906/indecs.17.1.3,

[22] Kiss, M. and Muha, L.: The *cybersecurity capability aspects of smart government and industry 4.0 programmes*.
Interdisciplinary Description of Complex Systems **16**(3-A), 313-319, 2018,
http://dx.doi.org/10.7906/indecs.16.3.2,

[23] NATO (2010): *Strategic Concept adopted by the Heads of State and Government of NATO member states in Lisbon for the protection and security of member states of the North Atlantic Treaty Organization. Active involvement, modern protection.*
https://2010-2014.kormany.hu/download/b/52/20000/nato_strategiai_koncepcio.pdf, accessed 27th May 2019,

[24] ITU (2017): *Definition of Cybersecurity*.
www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx, accessed 27th May 2019,

[25] ITU (2018): *Global Cybersecurity Agenda (GCA).*
www.itu.int/en/action/cybersecurity/Pages/gca.aspx, accessed 29th May 2019.

[26] ENISA (2017): *Cyber Europe.*
www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme, accessed 28th May 2019,

[27] ENISA (2018): *National/governmental CERTs Baseline Capabilities.*
www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities, accessed 30th May 2019,

[28] –: D*irective (eu) 2016/1148 of the european parliament and of the council.*
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, accessed 5th June 2019.