Security Challenges of Smart Meeting Rooms in Smart Cities

Bréda Gábor, ORCID:0000-0001-7868-6637
Óbuda University, Budapest, Hungary
bredagabi@freemail.hu

***Abstract*—The informatical development of our age is spreading in a more and more rapid pace. It is becoming impossible to find a physical environment, an area of around 10 square meters with no smart device or endpoint module in an urban environment. These devices that connect to the IT network usually serve a function that helps humanity. With the dynamic development of wireless IT technology we are in reach of more and more mobile devices that provide a more comfortable platform for today's most important activities: the flow of information and the control of comfort modules. These trends are highly followed in corporate environments, like offices and meeting rooms. Consequently, meeting rooms welcome HI-Tech equipment that provides an up-to-date visualization and communication. By setting up the new equipment we are facing new challenges concerning the security of information. As the subject of my research I am examining the communication equipment of today's meeting rooms from the point of view of information security, and will propose an optimum for presentation devices that is sufficient for the realization of a confidential meeting.**

I. INTRODUCTION

The technical development of our century has brought a degree of change to the life of mankind, which radically altered the daily life. The IT and communication systems' equipment completely entices itself into our lives, thus facilitating social contact with business and meeting the needs of our daily information needs. Since a large part of humanity lives in cities, it is obvious that the urban environment, as a living space, is beneficial to the spread of infocommunication technology, covering the entire living space. New types of service groups are emerging, offering the latest trends in information communication at affordable prices. [1]

The world's population is showing a steady growth. Apart from a separate analysis of ethnic groups and continents, according to the UN's statistical forecast, the current tendency predicts a population growth of close to two billion people over the next thirty years. The graph of this analysis is shown in Figure 1. Looking at the distribution of the population by habitat, also considering the statistics of the UN, the expected urbanization process predicts a proportional increase in the process of population growth. The expected evolution is illustrated in Figure 2, from which an interesting finding can be obtained regarding the increase in the number of rural population.

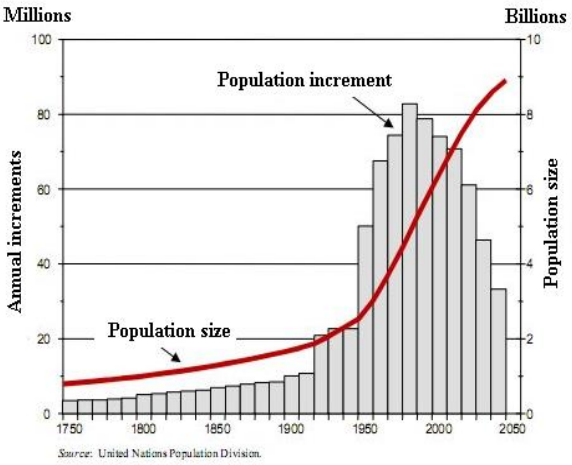

Figure 1. Long-term world population growth, 1750 to 2050
Source:http://www.science20.com/chatter_box/peak_oil_and_global_warming

The number of rural population will stagnate will show a somewhat declining value compared to the current situation. [2]

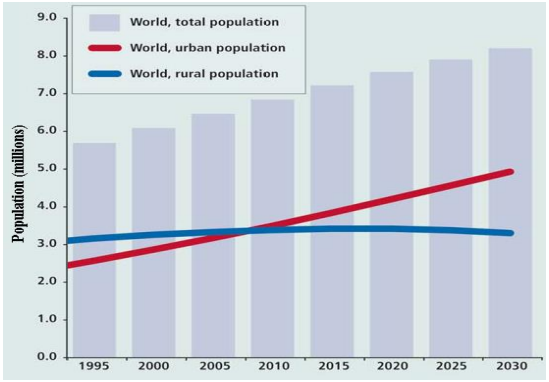

Figure 2- The urban and rural population of the world, 1995-2030
Source:http://www.un.org/esa/population/publications/WUP2005/2005wup.htm (2017.06.10)

Looking at the expected development of urbanization, we can examine the expected direction of development of the quality features of urban living space. It seems like a new technological process that can radically change everyday life. By coming to the subject of the article, it becomes a day-to-day reality that by covering cities with intelligent technologies, their living space will become a Smart City.

The wording of a Smart City is a tough task, but we can interpret it in the following way.
The definition of a Smart City as a concept stands for populated cities or settlements where information infrastructures and compatible communications technologies with full coverage and continuous operation are used in such a way as to promote a more diversified and more sustainable urban living space. Business investment in a modern information and communication infrastructure increases living standards and encourages sustainable economic growth while managing natural resources wisely. [3]
Basic providers that have a fundamental impact on quality of life continuously measure and monitor the parameters of their infrastructures. Parameters are stored in databases. Subsequently, the assessment of the values allows for deduction of conclusions that will give the inhabitants of the region an infrastructure that is more reasonable and enjoyable. Such infrastructures, for example, could be energy suppliers, transport providers, and companies providing services to cities. By 'smartening up' we can also mean that an element of a segment of the living space is constantly dependent on several other variables that always affect the values and processes that depend on it for the sake of reason and efficiency. The basic physical layer of intelligence has been provided by the infocommunication tools and channels. [4]
Showing all the elements of an entire smart vertical in a graph is a very difficult task, but if we talk about a smart city, we can think of the elements of Figure 3 below.

Figure 3. The components of a Smart City
Source:https://thenortheasttoday.com/nagaland-and-sikkim-cities-make-it-to-list-of-27-smart-cities/

The center of the smart city is the man and all that surrounds him serves the purpose of creating a better quality of life. Looking at the main elements of smart city, the first three elements of the following list can be considered as a primary concept for the subject, as this three-pronged driver demanded the measure that information should often remain confidential.

- Man
- Communication
- Economy, finance

- Transport
- Water management
- Energy management
- Urban Services

The following four sectoral elements, predominantly dependent on their first three functions, depend on the role of the first three decision-makers. Actually, man decides along economic interests and regulates the development of processes through communication.
Considering smart penetration, we cannot yet speak of a global collaborative network. Only the basis for smartening, the construction of a telecommunications network can be considered ready in a European context, which is, of course, not a small achievement. Smart solutions are still almost insulated for a particular technology. However, this trend is growing steadily and the proportion of interconnected networks is also increasing. Looking back on the development of telecommunication networks, a few years ago the possibility of mobile telephony or the number of internet access was possible only in islets. Most of it was tied to big cities and universities. Today in Europe, reviewing the coverage maps, we can observe that the vast majority of the continent has supply of both technologies. Nowadays, we can enjoy the benefits of a complex service on one device as one-off technology.
Looking at the Smart trend in the world, more and more cities are targeting the concept of smart city design. Based on 10 indicators, IESE Business School University has prepared the order of the world's smart cities. Among the aspects is human resources is the economic background of transport, urban planning, urban governance, technology, and social cohesion. The first three results per aspect are shown in Figure 4. [5] [6]

Figure 4. Ranking the world's smart cities by ten criteria
Source: http://www.ieseinsight.com/doc.aspx?id=1679

Expected appearance of smart devices will also affect your home environment. With reference to the results of a further research, taking into account US households, a 10 percent increase in the spreading of smart devices is expected in the next five years, as shown in Figure 5.

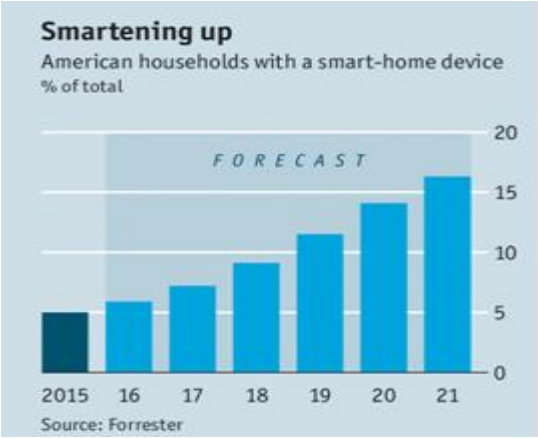

Figure 5. The growing number of smart devices in American households
Source:http://www.economist.com/news/business/21700380-connected-homes-will-take-longer-materialise-expected-where-smart (2017.06.10.)

Regarding the situation in Hungary, unfortunately we cannot speak of a real Smart City so far. Actually, only smart processes started, mainly in the form of energy and transport modernization. However, this situation may change. The Government's intention is to provide thousands of billion forints of funds through the exploitation of market and EU opportunities. At the end of 2014, a government decision was issued to prepare the concept of the Digital Nation Development Program and the Lechner Knowledge Center was appointed as coordinator of Smart City tasks. Within the Széchenyi 2020 plan, HUF 1231 billion is available for projects that fit into the concept of a smart city.
Looking at the practical implementation of the positive smart processes in Hungary, the "FUTÁR", the interactive information system of T-Systems Hungary in Pécs, or the Green City program in Szeged was launched in Budapest. [7] [8] [9] [10] [11].

II. HYPOTHESIS

Growth in population and the spread of infocommunication equipment can lead to particular assumptions in the context of smart cities and protected premises.
Communication technologies embody everyday life, generating new security challenges and solving suggestions.

Hypothesis I: As the population grows, the number of smart devices increases, together with the number of information security vulnerabilities created by smart electronic devices.
In order to protect the interests of vulnerability, there is still a need for confidential human-to-human communication.

Hypothesis II: While the entire volume of communication technologies is available to anyone today, as long as the content of human consciousness is not known by technology, the expression of people's thoughts is possible only through communication.

Hypothesis III: The spreading of Smart Devices and the implementation of encrypted areas create new expectations for a protected meeting rooms.
It may be the solution to ban smart devices from meeting rooms created to carry confidential human communication securely.

Hypothesis IV: An infocommunication-free environment reduces the risk of information leakage

Hypothesis V: Providing secured conversations with protected content requires the creation of a protected room along the lines of unified design principles.

III. THE CONTRADICTION OF SMART CITIES AND SECURITY

It is important to define the meaning of a few concepts on the subject, as they are used in more than one meaning in the everyday life.
A smart meeting room is a room equipped with technologies and techniques for direct human communication that meets the requirements of the age, with state-of-the-art IT equipment and technology elements combined with comfort, ergonomic functions for the most efficient and comfortable communication.
A protected area for the subject matter is defined as a demarcated area where sensitive, valuable data and information (at the authorized location, classified information and information) occur in any physical form occurring in human-to-human communication. The purpose of the protected premises is to ensure that the data and information that is available to the ones present and is available to the right-holders, is not accessible to unauthorized people, and the unauthorized acquisition of technology by all parties is not possible. The aim is to create and maintain uniform protection strength
Long-term forecasts regarding the spread of smart systems are a very difficult task, as new and more affordable equipment is emerging on a daily basis in the market with the continuous changing of trends.
By choosing the direction corresponding to my field of research I will have to separate the necessary measures into two parts to ensure safety. One is the human factor and the related level, the other is the technical level.
Human-level information protection is a separate area of research, but it can be strengthened by the protection of information, by law, and by various individual commitments and contracts. Such a source of law, for example, is the CLV law of 2009 on the Protection of Classified Data, which provides “the Parliament with the constitutional right to familiarize with public interest data and the possibility of limiting this right only in a necessary and proportional way, is about the protection of classified information”.

The primary source of data protection for the public sector at the technical level is the "law L. of 2013 on Electronic Information Security of Public and Municipal Bodies" [12] [13].
In addition to the laws, local information security regulations and measures protect the security of information, however, it can be said that a standardized or standardized solution for the protection of the spoken word or the negotiation of a protected content is currently not available in Hungary.
Protecting the oral information and connecting smart processes should address the security challenges posed by technologies. I am going to examine the security challenges of a room to be protected, where an employee in an office work environment discusses all relevant aspects of the company. As smart and information technologies are an integral part of our lives, so are the security risks that come with them have become a day-to-day problem in both the private and corporate environments.
By digging deeper into the subject, a new information security leakage gap seems to be emerging as a result of the fact that anyone has access to cheap, standalone, small voice and video capture devices. Their presence is also undesirable in protected environments. Information technologies have become indispensable in workplaces, but economic interests often require information confidentiality and protection. The smart meeting rooms of smart cities are creating a controversial situation in the aspect of creating security measures, as they follow trends in the propagation and deployment of information assets, while vulnerability increases proportionally. An additional device or system may have unforeseeable security vulnerability, causing unpleasant surprises to its users. Focusing on the topic, it is necessary to offer a solution to the exchange of information in a human-human context, in order to ensure safe communication. Social communication must be implemented in a secure environment that guarantees that the interaction of the communicating parties can only be observed by specific participants. Based on the known vulnerability of technologies, the trust and confidentiality of the involved parties is insufficient, therefore to create an exchange of information in a room where access to third party information is obtained, is necessary. Imagining the workplace environment covered by information and communication techniques, this protected, human-like information exchange can only be achieved in protected conference rooms. [14] [15] [16]

IV. SMART MEETING ROOMS AND EMERGING SECURITY PROBLEMS

Thinking about the subject, we are right to ask: What makes a meeting room smart?
Ergonomic and physiological design, comfort, and built-in visualization and infocommunication technology make a meeting room smart. The more and better the built-in technologies, the smarter it is.
By analyzing the communication functions individually, the priority is to easily share the content you want to present and discuss with audio and visualization technology. Here we can think of different projectors, smart boards and monitors. We can easily imagine that in the world of google glasses and 3D publishers we will soon be able to incorporate devices that are similar to those devices in the walls of the meeting rooms. In terms of their basic functions, they operate as a network terminal by requiring Internet as a basic operating condition. It is not enough to ensure the supply of energy; Internet is just as necessary of a basic service for the device to be able to reach the functions. The fast-paced world does not allow a large delay in negotiation waiting for remote decision-makers, so the feasibility of communicating with remote parties is also a key function of the built-in function of smart negotiators. In addition, the availability of all information communication technologies is a prerequisite for full wireless coverage and mobile technology. Negotiations often require a record, so basic sound and video recording is commonly used to create a studio-based device system. Comfort and ergonomic elements are highly emphasized in state-of-the-art meeting rooms, so we can rely on voice-controlled mechanical and shielding technology as well as climate control equipment.
If we are exclusively examining infocommunication techniques, we are confronted with the following technologies and the corresponding security vulnerabilities:

- Introducing Internet endpoints from an external room
- Wireless WLAN
- Conference equipment
- Hands-free unit - with studio
- Interpreting equipment - with studio
- Built-in video surveillance system
- Installed and portable computer
- Projectors, monitors
- Wireless conference room controller
- GSM coverage for all technologies

There are a lot of differences in the function of a meeting room and a protected room with the technology elements just mentioned. The safety of the protected room must be based on the principles of strength and control. In my opinion, a smart meeting room cannot really be a protected meeting room by incorporating technological trends. The information security approach of the protected meeting rooms should be approached in the following ways.

- physical security
- electronic information security
- document security
- security of the spoken word
- protection of displayed visual information

- protection of physical phenomena arising during communication

The first three of these possess established, ready-made, and protective solutions, but the protection of the physical effects created by the spoken word and the image that is being displayed and the appearance of these appear in the context of the above-mentioned needs. [17] [18] [19] [20]

V. THE OPTIMIZATION OF A PROTECED MEETING ROOM

Looking at the security vulnerabilities of the technologies used in smart meeting rooms, a protected meeting room can be a smart meeting room only in a limited way. Certain compromises should be made regarding the use of convenient solutions and the use of infocommunication technologies in meeting rooms.

Of the visualization solutions, only such devices can be brought between the walls of a meeting room that are controlled phisically, by a competent expert. There is no component in addition to the parts necessary for operation. The fact and validity of must be guaranteed.

Where possible, additional minimalization of technology is necessary for a protected room. There should be no way to reach a remote partner from between the walls of the room, since the creation of a such connection presupposes the presence of a data channel. Sound and picture recording functions are also undesirable in areas used as a protected meeting room.

In my opinion, some of the infocommunication technologies as well as the data transmission channels must be excluded from the enclosed security rooms, as the exclusion of the technology excludes the vulnerability it carries. [21] [22] [23]

Protected meeting rooms must meet the following requirements:

For secure communication, the room must be accessible in the normal work order. The schedule of maintenance and inspections must be carried out at times other than the working hours of the user group and the public must be excluded.

Considering the architectural design, and the tools and fixtures used in the meeting room, it is necessary to select them in a way that they can be clearly detectable, disassembled, and disposed.

The IT and infocommunication techniques required should be adequate for electronic information security.

All in all, the contents of discussions in the protected room must be kept between the walls and the consciousness of the participants. [24] [25] [26]

VI. COMMUNICATION ENVIRONMENT, RECOMMENDATIONS

As regards to the communication environment, we can talk about human-like analogue interfaces and physical phenomena created by publishers.

Such interfaces include loudspeakers, monitors, projectors, printers, and the writing itself of speech and drawing. Human-like phenomena by interfaces are sound wave, mechanical vibration, light, radio wave

The main aspect of the design of our protected room is that the physical phenomena appearing in the communication environment do not come beyond the walls of the room. If they are formed there, they should be attenuated inside and not detectable from the outside.

Using a meeting room, however, is often unimaginable with the use of a minimal number of technical equipment, so the following technologies can be applied by the use of limited solutions in the way I have imagined, with the convenience of a meeting room.

In protected areas, for the reasons outlined above, no network and Internet endpoints are suggested in any way, but you may still need a compromise solution. In this case, a temporary solution may be appropriate. An informatically and information security fueled line runs between the walls of the meeting room and it can be a good solution only for the necessary time. The introduction of wireless technologies into a protected room is, in my opinion, still unsuitable.

However, if a compromise solution is also required, the use of a type of technology of which the units do not generate radiations from the radio is useful. The placement of their components is to be placed between the walls of the protected room. Use of an external studio is not recommended. If an interpreter is required, it is also recommended that it be enclosed in the walls of the protected room, built in a way similar to a loudspeaker. For large rooms, the use of an infra-redundant interpreter equipment may prove to be appropriate. There is also a controversy about the use of protected meeting rooms and mobile phone technologies. In the presence of mobile phones, security can not be 100% in a protected conference room. We can easily eliminate this security gap by removing mobile phones from the walls of the protected room. For this, a good solution could be a mobile phone storage compartment outside the sheltered space. [27] [28]

In addition, further solution for minimizing threat would be to shield against radio waves and to overflow the radio environment of the room with radio interference. [29]

It is not recommended to install built-in video and sound monitoring and recording equipment in protected areas due to the inherent security risks. Therefore, only individually manageable recorders can provide a good solution if needed.

Moreover, in my opinion, there may be a risk to voice and remote controlled lighting, temperature, and windows, which are preferred in smart meeting rooms. In protected areas, simplicity should also be sought when designing the technical background of mechanical engineering and ergonomics. If possible, all unnecessary technical realizations should be omitted that make subsequent physical checks intransparent. Examining the recommendations from the point of view of furnishings and utensils, the principle of the required quantity must be followed. Items should be easy to overview. A good approach is the use of glass and plexiglass objects. Due to security vulnerabilities, there are concerns about the operation of computers in a protected meeting room walls. As managing presentations without the use of

computers is unsustainable, it may be a good idea to create a computer that does not have a stand-alone hard drive. The operating system works by running, for example, from a CD. The contents of the software will not be modified during use. The computer and auxiliary display devices must be magnetically shielded by attenuation of the radiation signal emitted by their operation.

New items will have to undergo technical content checks to avoid unwanted features. It is a general policy that if an object can not be checked, it should not, as far as possible, be taken between the walls of the protected room [30] [31].

As the basis of the defense method, here is the question of the design of a built-in basic model for the protected negotiators. I propose the principle as shown in Figure 6.

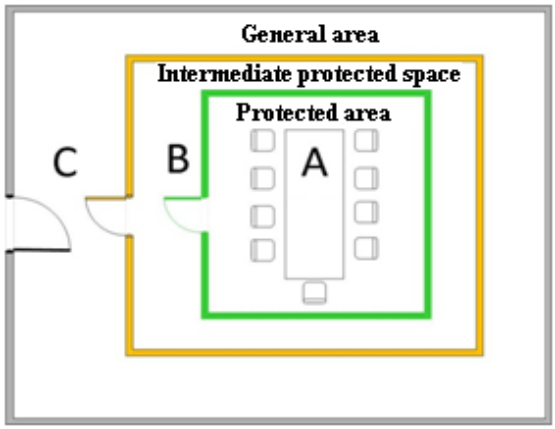

Figure 6. Dual walled protected room model (self-illustration)

In this arrangement, spaces "A" and "B" require a series of regime measures.

Zone A is a protected meeting room, Zone B is an intermediate protected space and Zone C is the part of the building surrounding the meeting room. The special environment is, as I imagine, the boundary walls of zones A and B including the floor and the ceiling. The boundary of the general building block is Zone C the outer wall of Zone B. Using electronic signaling and monitoring devices, it is necessary to provide a separate zone with a video enclosure covering the entire area of the outer part of wall B and provided with electronic property protection devices. The crossing points must be secured by a system of access while determining entitlements. A regime may be that only those operating the protected meeting room are premitted to enter Zones A, B, C. Only people arriving at the meeting may enter Zones A and C through doors and windows in section B, and only after special entry and personal check protocols, completely separating section B from the passing traffic, except for the doors and windows. Regarding the operation of the areas, it is not about using one room, but a complex system of areas built into one another. This is an unusual design, as conventional or smart meeting rooms do not require complete separation.

The task to be solved when developing a protected meeting room is to implement shielding against radio waves, as opposed to smart meeting rooms. The presence of full-featured wireless information technologies is the requirement of smart meeting rooms. The shielding of protected premises against radio signals has a dual function in creating information security that excludes the emergence of state-of-the-art wireless data connection from the meeting room walls and shuts the radio signals off from the electrical equipment, that are required to be used in the meeting room, from the outside world. By radio shielding we mean a technical solution in which the wall of the protected space is covered by some conductive layer. The model of Figure 6 illustrates a surface of wall B or C as well as doors and windows, making a Faraday cage. [32] [33] [34]

Looking for a range of real-world shading solutions and studying the range of manufacturers and distributors, I found a novel solution. On the market there is a special multilayer glass structure that loses transparency through electric current. By further developing the product, further coating of a shielding coating would provide a multi-layered glass that would make a number of architectural solutions simpler in the design of a protected room. The structural design of the glass to be formed is shown in Figure 7.

One of the coatings between the two layers of glass would obstruct transparency while the other would be to dampen the radio waves.

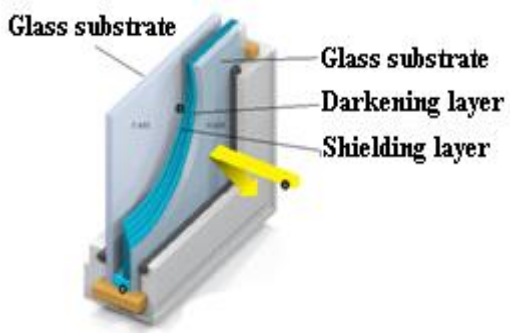

Figure 7. Multifunctioal glass
Source:http://fortune.com/2015/10/28/smart-windows/ [used of page figure]

Using this type of glass, I think it would be possible to create a meeting room that would satisfy most of the architectural and physical requirements. [35] [36] [37]

Speaking of the operation of protected area, only two words should come up about the operating personnel and the users. The operation of a such a room can only be a fiduciary activity. Maintaining a safe environment requires continuous instrumental inspection and periodic examination. Depending on the design of the room, different screening processes can be defined, forming an individual control protocol. The accessing of protected meeting rooms by the participants of the meeting requires additional personnel. Access must be secured by physical and instrumental inspection to the protected room to eliminate unwanted objects. [38] [39]

VII. CONCLUSION

Overall, smartening processes have started. When analyzing the design and operation of a protected conference room, there is a great contrast between smart meeting rooms and devices, and the sheltered conference rooms and their solutions. Protected areas should be designed and all of the aforementioned problems must be remedied one by one for reliable use. Keeping a good sheltered room or meeting room requires a different approach than today's trend. The control of the availability of information security needs to be kept in mind, putting technological advances in the background. Conscious preparation is necessary to overcome the information security gaps that emerge from smart urbanization. Protected areas must be object-protected buildings of controlled nature that have continuous protection and must be suitable for the exchange of sensitive discussion at any time beyond the maintenance period. There are solutions that can be used to construct areas that are protected from the point of view of the subject, which may prove to be adequate by excluding theoretical security vulnerabilities. Such spaces should be built in the future as they can be key to creating corporate information security. From the point of view of usage, in addition to the training of controlling personnel, users should be taught to maintain the level of protection as well as for the development of safety-conscious behavior for smooth operation.

REFERENCES

[1] Varga Péter János, "A kritikus információs infrastruktúrák értelmezése," HADMÉRNÖK III. évfolyam 2. szám, június 2008. pp. 149-156

[2] Enyedi György : A városnövekedés szakaszai újragondolva; Tér és Társadalom 25. évfolyam 1. szám, 2011. pp. 5-19

[3] "Smarter cityes for smarter groeth; How cities can optimize their systems for the talent-based economy" IBM Global Business service; Executive report,IBM Institute for Business Value, 2010.
Source:https://www.zurich.ibm.com/pdf/isl/infoportal/IBV_SC3_report_GBE03348USEN.pdf

[4] D. Tokody and G. Schuster, “Driving Forces Behind Smart City Implementations - The Next Smart Revolution,” Journal of Emerging research and solutions in ICT, vol. 1, no. 2, pp. 1–16, Dec.

[5] IESE Business School University, www.iese.edu IESE Cities in Motion IndexCenter for Globalization and Strategy
Source: http://www.iese.edu/research/pdfs/ST-0366-E.pdf

[6] IESE Business School University, " London Tops the Ranking of the World's "Smartest" Cities" Souce: http://www.ieseinsight.com/doc.aspx?id=1679

[7] Smart City 1.0 - Mérlegen a hazai városok okosodása
Source:http://k.blog.hu/2017/01/05/smart-city-hazai-varosok

[8] PAS 181 Smart City framework
https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/

[9] A Kormány 1631/2014. (XI. 6.) Korm. határozata a „Digitális Nemzet Fejlesztési Program” megvalósításáról Source:http://hirlevel.egov.hu/2014/11/08/a-kormany-16312014-xi-6-korm-hatarozata-a-digitalis-nemzet-fejlesztesi-program-megvalositasarol/

[10] A Kormány 1486/2015. (VII. 21.) Korm. határozata a Digitális Nemzet Fejlesztési Program megvalósításával kapcsolatos aktuális feladatokról, valamint egyes kapcsolódó kormányhatározatok módosításáról
Source: http://hirlevel.egov.hu/2015/07/21/a-kormany-14862015-vii-21-korm-hatarozata-a-digitalis-nemzet-fejlesztesi-program-megvalositasaval-kapcsolatos-aktualis-feladatokrol/

[11] BAUMAN,Z. Globalizáció. A társadalmi következmények. Szukits Könyvkiadó 2002

[12] "2009. évi CLV. törvény A minősített adat védelméről" Source:https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0900155.tv

[13] "2013. évi L. törvény Az állami és önkormányzati szervekelektronikus információbiztonságáról"
Source:http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.tv

[14] Ványa László; Zrínyi Miklós Nemzetvédelmi Egyetem, Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre, Doktori (PhD) értekezés, 2001

[15] Haig Zsolt Az információbiztonság komplex értelmezése, ZMNE Hadmérnök különszám, Robothadviselés 6

[16] Kerti András, " A vezetési és információs rendszer technikai alrendszerének vizsgálata különös tekintettel a minőségbiztosításra és az átvitelbiztonságra," doktori PhD értekezés 2010. Témavezető Prof Dr. Rajnai Zoltán mk. ezredes egyetemi tanár

[17] Muha Lajos, A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, Doktori értekezés, Budapest 2007. Tudományos vezető Dr. Kovács László mk. őrnagy PhD egyetemi docens

[18] Haig Zsolt, "Az információs társadalmat fenyegető információalapú veszélyforrások, "Hadtudomány, XVII. Évfolyam 3. szám 2007. szeptember

[19] Prof. Dr. Rajnai Zoltán," Információbiztonság tudatosság," In: Bitay Enikő (szerk.) A XXII. Fiatal Műszakiak Tudományos Ülésszak előadásai: Proceedings of the XXII-th International Scientific Conference of Young Engineers. 418 p. Konferencia Kolozsvár, Románia, 2017.03.23-2017.03.24. Kolozsvár: Erdélyi Múzeum Egyesület (EME); Óbudai Egyetem, 2017. pp. 37-43.(Műszaki Tudományos Közlemények - Papers on Technical Science; 7.) (ISBN:978-963- 449-018-0)

[20] Rajnai Zoltán, Fregan Beatrix Kritikus infrastrukturák védelmeIn: Bitay Enikő (szerk.)A XXI. Fiatal Műszakiak Tudományos Ülésszaka előadásai. [Proceedings of the XXI-th International Scientific Conference of Young Engineers]. 452 p. Konferencia helye, ideje: Kolozsvár, Románia, 2016.03.17-2016.03.18. Kolozsvár: Erdélyi Múzeum-Egyesület (EME), 2016. pp. 349-352.(Műszaki Tudományos Közlemények - Papers on Technical Science; 5.)A XXI. Fiatal Műszakiak Tudományos Ülésszaka előadásai - Proceedings of the XXI-th International Scientific Conference of Young Engineers

[21] Vadász Pál, "Információkeresés a gazdasági hírszerzésben," Hadmérnök IX. évfolyam 2. szám - 2014. június. pp. 343-357

[22] Környei Mátyás, "Üzleti titokvédelem," Pécsi Tudományegyetem Állam- és Jogtudományi Kar Óriás Nándor Szakkollégium Scriptura ISSN 2064-7646; 2015. I. szám pp. 170-185

[23] Dr. Keszthelyi András "Információbiztonság, technikai alapismeretek" OEKGK Szervezési és Vezetési Intézet, Vállalkozásfejlesztés a XXI. században, Budapest 2012. pp. 303-340

[24] Critical Foundations Protecting America’s Infrastructures, The Report of the President’s Commission on Critical Infrastructure Protection, Washington, 1997. október
https://fas.org/sgp/library/pccip.pdf

[25] Précsényi Zoltán, Solymosi József, "Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé," Hadmérnök II. Évfolyam 1. szám 2007. március pp.65-76

[26] Kuris Zoltán," Komplex információbiztonság megvalósítási lehetőségeinek megközelítése," Hadmérnök IV. évfolyam 2. szám 2009. június pp. 311-318

[27] Végvári Zsolt, "A lehallgatás ellen védett mobiltelefonálás összehasonlító vizsgálata," Katonai logisztika 22. évfolyam 2014 II. szám. pp. 146-170

[28] A Nemzeti Biztonsági Felügyelet feladatairól és az elektromágneses kisugárzás elleni védettség minősítéséről http://www.nbf.hu/tempestmer.html (letöltve: 2017.01.06)

[29] Berek Tamás, "ABV (CBRN) analitikai laboratórium beléptető rendszere a biztonságos üzemeltetés szolgálatában," Hadmérnök, VI. Évfolyam 2. szám, 2011/2, ISSN1788-1919, pp. 21-36

[30] Haig Zsolt, Várhegyi István, "Hadviselés az információs hadszíntéren,"Zínyi Kiadó, Budapest, 2005; ISBN9633273919

[31] Boros Béla, Bottyán Róbert, Dessewffy Sándor, Koskovics István, Kovács József, Liszt Ferenc, Móró Lajos, dr. Szili László, "Rendészet, vagyonvédelem," BME Mérnöktovábbképző Intézet 1997; ISSN 08653313, ISBN963-431-797-9ö,801-0

[32] Dr. Töltési Imre, "Lehallgatás védelem az üzleti szférában 1," Detektor plus 2006.07. pp.32-33

[33] Dr. Töltési Imre, "Lehallgatás védelem az üzleti szférában 2," Detektor plus 2006.08-09. pp.58-59

[34] Dr. Töltési Imre," Lehallgatás védelem az üzleti szférában 3,"Detektor plus 2006.10-11. pp. 47-49

[35] Vaszari Ádám, "Üzleti hírszerzés a multinacionális cégeknél és a kis és közép állalkozásoknál," Diplomamunka BGF-KFK, Budapest, 2007

[36] Berek Lajos, " Biztonságtechnika," ÁROP 2.2.21 Tudásalapú közszolgálati előmenetel Nemzeti Közszolgálati Egyetem, Budapest, 2014

[37] Berek Lajos, Berek Tamás, Berek László, "Személy és vagyonbiztonság," ÓE, Budapest, 2016, ISBN 978-615-5460-94-4

[38] Lazányi Kornélia,"A biztonsági kultúra," TAYLOR Gazdálkodás- és szervezéstudományi folyóirat 2015. 1-2 szám;Szeged 2015, pp. 398-405

[39] Lazányi Kornélia, "A biztonsági kultúra szerepe a vezetői döntések támogatásában," TAYLOR Gazdálkodás- és szervezéstudományi folyóirat 2016, 1. szám; Szeged 2016, pp. 143-150