HADTUDOMÁNYI SZEMLE

2017. X. évfolyam 3. szám

IMRE DOBÁK[1]

Surveillance, information gathering – changing environment

Megfigyelés, információgyűjtés – változó környezet

Abstract

The purpose of this paper is to provide insight to the changes of surveillance and technical type of information gathering that have occurred at international level over the past time, and to highlight the importance of the topic. Nowadays, the changes related to this issue are extremely dynamic, because the governments and their national security services and law enforcement organizations have been trying to give prompt answers to those challenges, risks and threats that negatively affected the security.

Keywords: security, surveillance, secret information gathering

Absztrakt

Jelen tanulmány célja, hogy rávilágítson a technikai típusú információgyűjtés, megfigyelés jelentőségére, és az elmúlt időszakban nemzetközi szinten lezajlott változásokra. A kérdéskörben látható változások napjainkban rendkívül dinamikusak, hiszen a biztonságot negatívan befolyásoló kihívásokra, kockázatokra, fenyegetésekre a kormányok (és biztonsági szervezeteik) igyekeztek rövid időn belül válaszokat adni.

Kulcsszavak: biztonság, megfigyelés, titkos információgyűjtés

INTRODUCTION

In the recent years, significant changes have taken place in the information gathering and lawful interception of national security and law enforcement services. The previous traditional, technical type of information gathering solutions and methods have changed accord-

[1] Nemzeti Közszolgálati Egyetem, egyetemi docens - National University of Public Service, Associate Professor, E-mail: dobak.imre@uni-nke.hu, ORCID: 0000-0002-9632-2914, The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance” in the Miklós Zrínyi Habilitation Program.

ing to the technical environment and security challenges, so the concerned organizations have taken steps to revise their capabilities, practices and laws. The cyber and the technical nature surveillance have become more important and the usage of these indispensable capabilities has increased. Their existence and application nowadays are widely known too, because of the legal frameworks and also due to the Snowden revelations[2] (2013).

All these changes make it worthwhile to review briefly the topic, and highlight its importance. The examination of the subject relies on such international public sources where we mainly meet with the legal approaches of information gathering (e.g. regulation of national security / law enforcement) and right to privacy or with the questions of increasingly dominant cyberspace. The issue can be considered to be highly multidisciplinary after its close examination, different areas of technical-, social-, and legal sciences may also appear.

There are two main factors behind the relevance of the topic: namely the intensified intelligence and security information needs related to terrorism threats, and the emergence and lawful applicability of the new information gathering capabilities (methods) in the technological environment. Looking out the European scene and excluding the national security or law enforcement differences, this paper intends to have a brief overview of some relevant points of the topic.

SOME ASPECTS OF THE ISSUE

It is worth to emphasize that legal regulations - including the national level rules for surveillance practices for both law enforcement and national security - are highly complex and different in some details. It is also a fact that (secret) information gathering for the purposes of the national security (intelligence) is not to be confused with the lawful interception[3] of assigned authorities acting for law enforcement (e.g. police) purposes. Even though there might be some similarities related to technical skills and methods, but their tasks – e.g. concerning the levels of security issues and interests - are different. Rules of information gathering also may show differences between law enforcement and national security practices in respect of different countries. On this field, the phenomenon of terrorism as a specific threat encouraged to rethink the surveillance practices and its legal background in the digital era. In the background, there is also a wide range of social debates about the question of security vs. protection of fundamental rights. These are well reflected in the related international documents, in the scientific analyses and statements appearing on the political scene.

[2] See: The Guardian, NSA files: Decoded, available at: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (accessed August 21, 2017)

[3] „Lawful interception (LI) is a security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organizations." Cited from: http://www.etsi.org/technologies-clusters/technologies/lawful-interception (accessed August 10, 2017)

In the meantime, the information and communications technology (ICT) is constantly evolving, due to the Internet, it is by its nature, a cross-border phenomenon. Cyberspace comes to the forefront, it gets a new interpretation concerning the challenges, risks and threats that affect security and it requires proper responses from security agencies. It is also a fact that ICT is a decisive factor in the whole society, which besides to peaceful-minded people is also open[4] to both national security threats and illegal activities.

In the changing security environment, the threats come from unpredictable locations, from national territory or from remote geographic areas. Let's just think to the intensifying terrorism[5], the organized crime, the various areas of cybercrime or even the emergence of some economic and financial problems. The other side of the coin is that, these problems demand prompt actions of law enforcement agencies and security services in surveillance, lawful interception and the cybersecurity activities.

KEY ISSUES OF THE PAST YEARS

In recent years, the effects of security policy events, the technological advancement or the national security leaks[6] have highlighted several key factors as well. This publication is intending to outline them below.

— *Leaks:* The US intelligence scandal emerged in 2013 revealed that the technical capabilities of our age allow bulk information gathering regardless of state or geographical boundaries.[7] It has raised several debates including the surveillance in the expanding cyberspace, the role of the state in protecting its national security, the place and role of corporate actors and last but not least, the issues of the right to privacy.

— *Expansion role of cyberspace:* After the turn of the millennium, the security needs related to the cyberspace has expanded and became dominant. It has created new challenges as the ground of "information gathering" / "lawful interception" and as a place of cybersecurity for the state and other actors. It can be seen from pub-

[4] Boda J. - Dobák I.: A technikai-műszaki nemzetbiztonsági szolgálatok és feladatok jelentősége a 21. században, In: Boda József, Dobák Imre (ed.) A nemzetbiztonság technikai kihívásai a 21. században, Bp., NKE Szolgáltató Nonprofit Kft, 2015.

[5] The use of the Internet for terrorist purposes, United Nations Office on Drugs and Crime, Vienna, UN, September 2012., available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (accessed July 15, 2017)

[6] See wikileaks (e.g. Vault 7, or Spy Files) documents, available at: https://wikileaks.org/+-Intelligence-+.html

[7] We have seen examples not only by the NSA (US), but in the UK (GCHQ), in Germany (BND) or "*the French DGSE has allegedly placed … interceptors on underwater cables out of its military base in Djibouti*". See: Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, R. B. J. Walker; After Snowden: Rethinking the Impact of Surveillance, International Political Sociology, Volume 8, Issue 2, 1 June 2014, p. 121–144, https://doi.org/10.1111/ips.12048

lic sources as well that concerning the cyberspace as a new conflict zone many countries have formed their strategies and organizations for cyber issues (e.g. cyber security, cyber intelligence...).

The open nature of the Internet and the cross-border nature of infocommunication systems are the key factors for security organizations, where it is often difficult to determine where the relevant threats come from. Managing these threats can often go beyond the state, for example at the theme of counter-terrorism, where the cyberspace has a special relevance. (As the related UN document defined *"the Internet is often utilized to promote and support acts of terrorism", as for "propaganda (including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyberattacks.")*[8]

— *Regulatory environment:* Nowadays, it is commonly known that in democratic countries, the national security services are oversighted and controlled by external control mechanisms and the frameworks for the secret information gathering were codified in laws.[9] Legitimate and legally permitted interception of telecommunication systems is present on the European stage since 1995 in accordance with the resolution of the EU Council. This decision states that *„the legally authorized interception of telecommunications is an important tool for protecting the national interest, especially in case of national security and investigation of serious crime"*[10]. In addition to the national legislation, international technical standards were developed and have taken steps to follow the changes of technological environment (e.g. cloud[11]). The European level for the development of the international standards of lawful interception reinforced the same technological bases of surveillance capabilities as well as the accountability thereby indirectly strengthened the protection of privacy. Standards also operate as links to the infocommunication companies, setting a specific framework for cooperation. The standards of ETSI (Eu-

[8] The use of the Internet for terrorist purposes. United Nations Office on Drugs and Crime, Vienna, UN, September 2012. p.3. available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (downloaded August 15, 2017)

[9] See: Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében, Hadmérnök XII/2, 2017. p. 236, availableat: http://hadmernok.hu/172_19_dobak.pdf (downloaded: July 15, 2017)

[10] Council Resolution, of 17 January 1995 on the lawful interception of telecommunications, (96/C 329/01), Official Journal of the European Communities C 329, 4.11.1996. Volume 39, ISSN 0378-6986 http://eur-lex.europa.eu/legal-content/EN/TXT/%20PDF/?uri=OJ:C:1996:329:FULL&from=EN (downloaded: July 15, 2017)

[11] Lawful Interception (LI); Cloud/Virtual Services for Lawful Interception (LI) and Retained Data (RD) available at: http://www.etsi.org/deliver/etsi_tr/101500_101599/101567/01.01.01_60/tr_101567v010101p.pdf (accessed July 15, 2017)

ropean Telecommunications Standards Institute) can provide a consistent interpretation between service providers and law enforcement or even national security authorities. ITU (International Telecommunication Union) also draws attention to the need for law enforcement technologies based on the exact international standards.

— *Data collecting:* Following the Snowden case, a wide range of studies examined the issues, and outlined some important focus points: the question of the mass data surveillance[12], the issue of domestic and foreign data collection[13], the complexity of national security and law enforcement information gathering as well as the social sensitivity related to information gathering. In the case of metadata[14], the question of collecting, storing and also the ability of processing them has raised some problems considering the fact that without being analysed and evaluated, these data are basically only data sets. As the UN General Assembly (2016) noting *"while metadata can provide benefits, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity"*. It is a question that after analysing these mass data, how deep it may violate the rights of privacy of a given person as detailed information can be obtained about his habits and behaviour.[15]

— *Encryption:* Nowadays, the new encryption solutions are widely available not only for the state actors, but also for business and people. On the other hand, its widespread use has a determining affect to the effectiveness of the surveillance. In the beginning of this century, the governments' organizations carrying out their lawful interception and information gathering tasks have already met with a growing technical level of encryption[16], where the service providers were increasingly re-

[12] Concerning the meaning of „mass surveillance" it is worth to quote the mentioned EU study: *„It refers broadly to the bulk access and/or collection of many users' communications without prior suspicion of individual targets. Therefore, mass surveillance involves no individual target, no prior suspicion, is not time bound and due to the technology employed, potentially limitless."* Cited from: Susan Morgan: "Lawful Interception and Government Access to User Data: Designing a Rights-Respecting Model" (Jan. 2016). IHRB p.7.

[13] Often cited source is the PCLOB (Privacy and Civil Liberties Oversight Board) Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (US practice) (2014) which describes in detail the two-main type of foreign PCLOB information gathering („downstream" and "upstream"), available at: https://www.nsa.gov/about/civil-liberties/resources/assets/files/pclob_section_702_report.pdf (accessed: May 20, 2017)

[14] The metadata means the non-communication data (e.g. number, e-mail address, location, time, network, service provider, etc.)

[15] Concerning the UK Investigatory Power Bill see Glyn Moody writings. Available at: http://arstechnica.co.uk/tech-policy/2016/11/investigatory-powers-act-privacy-disaster-waiting-to-happen/ or https://arstechnica.co.uk/tech-policy/2016/03/revised-snoopers-charter-ignores-key-criticisms-widens-police-powers-further/(accessed: May 20, 2017)

[16] In Europe, the attention was focused to the encrypted communications after the terrorist acts (2015) in Paris, assuming that it could be particularly suitable for concealing information between terrorists

luctant to support governments' secret requests for data as well. Due to the challenges caused by encryption, and the failure of lawful access to information (Going Dark[17]) there has been an increasing pressure on the state security organizations. In the field of responses, as a special example, the previous US practice could be mentioned, when they took steps to hold its decoding capabilities (e.g. a " key escrow" system[18]). But in the recent years, the specific information gathering solutions (e.g. hacking) come to the fore more likely, or the co-operation with service providers gets a greater role.[19]

— *Providers-Corporate actors:* Nowadays, the providers bear an indispensable part in surveillance, since a huge bulk of data and the communication itself can be found in the system of infocommunication service providers[20]. Their development activities are continuous and extremely fast, moreover their interests are influenced by economic factors. Geographically, many of their services are cross-border (e.g. Internet and Internet-based services), but their co-operation obligations are basically based on (national) laws, which can result imbalances. They are in an intermediate role in information gathering/lawful interception cooperation with the states. On one hand, their co-operation is extremely important for the security agencies performing the duties of governments, and on the other hand, as a provider, its duty is to protect the communication of their users (right to privacy). Cooperation may also have some negative business impacts, and it may lead to reduce the users' confidence in service providers: e.g. the users will not use the

before the authorities. The “encryption” debate came to the fore in 2015, when some major communications services providers have enabled to use the end-to-end encryption in their applications. See: Don’t Panic, Making Progress on the “Going Dark”, Debate February 1, 2016, The Berkman Center for Internet and Society at Harvard University, available at: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf (access: August 25. 2017)

[17] See: James B. Comey: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? October 16, 2014 available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf (access: August 05. 2017)

[18] See: Mirja GUTHEIL, Quentin LIGER, Aurélie HEETMAN, James EAGER, Max CRAWFORD: Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, European Union, 2017, p.18.

[19] Some intelligence services ... work on a very large scale and use voluntary or forced collaborations with private providers … and telecommunication companies”. See: Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, R. B. J. Walker; After Snowden: Rethinking the Impact of Surveillance, International Political Sociology, Volume 8, Issue 2, 1 June 2014, p. 121–144, https://doi.org/10.1111/ips.12048

[20] As the UN General Assembly (2016) notes: "that the increasing capabilities of business enterprises to collect, process and use personal data can pose a risk to the enjoyment of the right to privacy in the digital age". See: UN General Assembly, 16 November 2016 A/C.3/71/L.39/Rev.1, available at: https://www.accessnow.org/cms/assets/uploads/2016/09/privacy-resolution-2016-UNGA.pdf (downloaded: 2017.08.22.)

technology if they do not trust in its security (see: technology trust deficit).[21]. In recent years, we have seen many examples of these, let's think of the cooperation between IT service providers and security agencies in the mass data collection of the US, or as a counter-example the rejection of security service providers' request by the service providers (using encryption, Apple vs. FBI).

— *Privacy*: Members of the society necessarily use communication technologies in their daily lives and to protect their privacy is a basic requirement. Nevertheless, among the peaceful minded members of the society, those ones can also be present who threaten the security of the nation (criminals, terrorists), so their presence requires the response of the security forces. In the last third of the 20th century, we could see the coming into force of the public regulations of secret services, the strengthening of the external overview system in the democratic societies and also the debates about the surveillance vs. protection of privacy.

The regulated state level of information collection has been already widely accepted by the society, but debates about the extent of information gathering often arise. As it is in the above cited relevant EU study, the law protects the private communications but *„… in specific and defined circumstances, such as those related to national security threats or other narrowly defined situations of public safety or crime prevention, governments may legitimately restrict the right and intrude on individual privacy provided a number of specific conditions are met.”*[22] It is a fact, that the surveillance activity must have a comprehensive legal and professional framework, along which - according to democratic standards - the relevant national security and intelligence organizations can operate and perform their activities. The UN General Assembly has already called upon the States in 2016: *"to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law".*[23]

As a specific phenomenon, the periodic shift of social sensitivity concerning the secret organizations could also be observed. This attitude may change when such an event happens which has a negative impact on security (the European terrorist acts of recent years might serve as good examples). After these events, the secu-

[21] See: KRIS, D. S. (2016). Trends and predictions in foreign intelligence surveillance: The FAA and beyond. Journal of National Security Law & Policy, 8(3), p.6 https://search.proquest.com/docview/1831706283?accountid=42933

[22] Susan Morgan: “Lawful Interception and Government Access to User Data: Designing a Rights-Respecting Model” (Jan. 2016). p.11.

[23] 16 November 2016 A/C.3/71/L.39/Rev.1, available at: https://www.accessnow.org/cms/assets/uploads/2016/09/privacy-resolution-2016-UNGA.pdf(downloaded: 2017.08.22.)

rity needs of the society (and state) and also the role of potential information gathering on technical field can increase and it may even affect the activity and structure of the concerned organizations.

RESPONSES TO CHALLENGES IN OUR DAYS

As an obligation, the states have to guarantee the national security of the concerned country. Along their tasks, it may appear the information needs of law enforcement agencies and national security that can use information gathering activities including technical elements as well. This activity is not new on the European stage and - irrespective of any political systems - their application goes back to the beginning of the 20th century. However, beyond the traditional forms (e.g. wiretapping), the actual information gathering solutions can be largely related to cyberspace. The protection of privacy on the surveillance / secret information gathering stay important. As the Institute for Human Rights and Business defines *"Intercepting or monitoring communications is an intrusive process into someone's privacy and therefore a strict legal framework should govern such actions to prevent arbitrary violations of rights such as privacy and freedom of expression"*.[24]

RESPONSES:

The task of the national security services is to respond efficiently to different threats along their lawful operations, their tasks and their capabilities, meanwhile they take into account the constantly changing technical environment and they also provide the necessary information through their secret (and open) information gathering activities.

- Actors in the technological environment are facing with masses of information (Big Data). The everyday lives of users have been intertwined with digital communication and a huge amount of (offline and online) data arises because of it. This information set contains also those data which can help the authorized security organizations to achieve efficiently theirs tasks. Thus, these organizations understandably take steps to use the modern surveillance and interception technologies. While the most up-to-date tools are being used for illegal activities, the national security organizations have to be prepared in long-term to create their lawful interception capabilities.
- After 2013, the defense against the intelligence of other states amplified the defensive reflexes of European states (e.g. cyber security) at first and the issue of data protection (e.g. Safe Harbor[25]) became a priority. In the meantime, the terrorist acts occurring in Europe highlighted the importance of applying the modern

[24] Susan Morgan: "Lawful Interception and Government Access to User Data: Designing a Rights-Respecting Model" (Jan. 2016). p.6.)

[25] What is 'safe harbour' and why did the EUCJ just declare it invalid? available at:https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection (downloaded: August 06, 2017.)

surveillance technologies in relation to the tasks of state security services. Several countries across Europe have reviewed their relevant rules and have taken steps to increase their applicability in the fight against terrorism.[26]

— Security threats, challenges and also the evolving technological environment have enhanced the significance of national and international level cooperation as well. Regarding the gathering information, it is clear that serving information needs have already been closely linked to the external infocommunication environment. At international levels, it became visible a more effective response to the cyber threats (increased cyber security).

— The wide range of corporate environment helps to operate and develop the governments' surveillance solutions with its infocommunication-based developments. All of these are present in both national security and law enforcement tasks. Due to the use of modern technologies and the necessary specialists and also by reason of other respects, the companies often support this field as an outsourcing ac-

[26]The revision of the national legislation of secret information gathering in Europe has begun as a result of the recent terrorist attacks in Europe. For example:

- In the United Kingdom, it has come to the fore that the intelligence services should get more possibilities[26] to fight against terrorism in 2015.[26] There was an extended professional debate before the Investigatory Powers Act, which aimed mostly at the telephone companies and Internet Service Provider, to create the obligation to store (for a year) the so-called Internet Connection Records (ICRs) in order the relevant security services could have access to the records upon request. Some opponents attacked it because of their extremely wide licenses. The government, however, had maintained its vision and the law was adopted at the end of 2016 as the main legal basis for the surveillance by law enforcement and the security and intelligence services. See: MOODY, Glyn - 17/11/2016, Why the Investigatory Powers Act is a privacy disaster waiting to happen, http://arstechnica.co.uk/tech-policy/2016/11/investigatory-powers-act-privacy-disaster-waiting-to-happen/ (downloaded: April 25, 2017) or GRIFFIN, Andrew: Snoopers' Charter: Theresa May to push huge new spying powers through Parliament, despite major report concluding they are not needed, 11 June 2015 http://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-theresa-may-to-push-huge-new-spying-powers-through-parliament-despite-major-report-10313042.html (downloaded: July 10, 2017)
- In Russia, the year of 2016 was also a turning point in the issue of information gathering based on Internet technology. According to media sources, in the country, in the mid-2016, several anti-terrorist laws amendments were approved. The anti-encryption and data retention law (Yarovaya Law) deal with those telecommunications providers, that have to store all telephone conversations and text messages for six months, and the metadata of calls for three years.[26] The "organizers of information distribution on the Internet" (so web resources) have to store the information for one year. Under the Law "organizers of information distribution on the Internet" (e.g. websites messenger apps, social networks, e-mail clients) that encrypts their data, "*are required to help Russia's Federal Security Service decipher any message sent by its users."* Ronald Bailey: Is Russia's Surveillance State Being Modelled on the West?, New Russian anti-encryption and data retention laws look sadly familiar. Jul. 22, 2016, reason.com, available at: https://reason.com/archives/2016/07/22/is-russias-surveillance-state-being-mode/print (downloaded: April 30, 2017), and the "Russia's State Duma just approved some of the most repressive laws in post-Soviet history", Meduza, 24 June 2016, available at: https://meduza.io/en/feature/2016/06/24/russia-s-state-duma-just-approved-some-of-the-most-repressive-laws-in-post-soviet-history(access: August 18, 2017)

tor in many areas. This means a specific relationship and association (e.g. economy factors, reliability issues, availability of development capacities, and involvement of international corporate actors).

- A specific technology industry[27] has been built to provide those surveillance and lawful interception technologies, which are expected to be developed. The related market publication[28] defines "„global lawful interception market is expected to garner $2.1 billion by 2020”. This specific market area targets the governments and security organizations with its lawful interception/ surveillance solutions. Concerning the technological developments, besides the traditional solutions, the cyber space is one of the most important segments. The market is rapidly growing and this is expectedly will continue. One of the reasons of the development is that more and more countries in the world are using industry-specific solutions for "lawful interception". Because of the fight against terrorism and the spread of cybercrime, the countries and governments are modifying their legal environment, and thus they have the opportunity to apply such advanced technology solutions.
- Concerning the encryption issue, it is a subject of international debates that, in spite of the need for strong encryption, there is also a huge demand to resolve the issue that the law enforcement or national security services would have access to the data they need. Based on the reviewed source, the disputes concern the security vs. private life. In the literatures, it stated that, on the one hand, the enforcement of new technical solutions serves the increase of security; but on the other hand, some civil actors may also perceive a potential threat to privacy.
- Encouraging the encryption, as a study[29] reveals, *"remains strong in international and EU forums"* and also a 2017 report[30] emphasizes protection of individuals' online security. On the political level, it appears among the dominant thoughts, supporting strong encryption standards with regard to the privacy of members of civil society. However, the European terrorist acts of recent years have brought again the issue to the focus of attention. In 2012, a related UN publication have already put, that terrorists may use the Internet for preparatory secret communication, and they "have become increasingly sophisticated at exploiting communica-

[27] In general, it can be stated that the different intelligence technologies basically are not different from the technologies used in the "civil" environment. These cannot be separated from the development of technical environment, and the differences can be searched related to their intended purpose and their specific applications.

[28] See: https://www.alliedmarketresearch.com/lawful-interception-market

[29] See: Mirja GUTHEIL, Quentin LIGER, Aurélie HEETMAN, James EAGER, Max CRAWFORD: Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, European Union, 2017, p.18.

[30] UN General Assembly, A/HRC/35/22, 30 March 2017, Human Rights Council Thirty-fifth session Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, p.6. available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement (access: August 17, 2017)

tions technologies for anonymous communication related to the planning of terrorist acts."[31]

The question is that, if the concerned governments and their organizations are not able to access to the decrypted communications directly then what kind of other lawful possibilities do they have to get the information they need? The law enforcement organizations therefore could turn to different hacking techniques in the ICT area.[32] Looking at the processes of recent years, it is clear that such kind of specific techniques start to become determinant in the field of law enforcement (or even national security) gathering of information.

Besides the legislative procedures, often come up the questions, that who develop these new surveillance techniques[33] and methods. In the European scene neither all governments, nor their law enforcement or intelligence / security services have capabilities to develop such techniques.

— The security agencies have searched for new, legally applicable solutions, technical options as they also have taken steps to change the legal environment to ensure their monitoring and control capabilities. Legislative changes of the international scene over the past period have served increasingly this process and its efficiency.

[31] The use of the Internet for terrorist purposes, United Nations Office on Drugs and Crime, Vienna, UN, September 2012., https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf 10.p

[32] The mentioned study (Mirja Gutheil, Quentin Liger, Aurélie Heetman, James Eager, Max Crawford: Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, European Union, 2017) dealing with the "hacking" issue in lawful interception, defines that France, Germany, Poland and the UK have already adopted specific legislative provisions and in Italy, and in Netherlands these are in process. The study also points out that:

- In France in the middle of 2016, the law enforcement agencies were allowed to have remote access to computers and other devices.
- In Italy, the law enforcement has been using the hacking practices for years, and in February 2017 a new legislative bill draft was presented.
- In Poland, the law enforcement agencies (according the amendments to the Police Act) have *„the power of covert access to information systems”*, since 2016.
- In Netherlands, also is in progress the Computer Crime III Bill, (as called Hacking Law) which *„aims to regulate the use of hacking as an investigative power…”*.
- In France, the authorities *„have developed in-house tools for remote access. However, as technical investigative tools must be legally authorized, this process took time.”*

[33] We can see the Germany example where *„BKA no longer purchases external hacking expertise but intends to develop its own tools”,* what's more the Ministry of Interior established a new authority for provision of technical skills and expertise. In Italy the draft law *„states that trojans must be operated by in-house personnel and not private contractors.”* (See: Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, European Union, 2017)

CONCLUSIONS

- The widespread use of advanced infocommunication tools (smartphones, computing devices) during the illegal activities affect the development of surveillance directions and methods. Governments necessarily use the new information methods and in the fight for security, can no longer rule out the application of these technologies.
- The secret information gathering organizations, whether they are national security services or law enforcement agencies are forced to be in constant development by the evolving info communication environment. All these can be traced in the legislative debates and processes as well. Nevertheless, it is the task of the governments to find the balance between upholding the right to privacy and promoting the security of the society.
- The meanings of the boundaries are re-evaluated by the role of cyberspace and by the presence of multinational telecoms providers. It became possible (for national security services) to provide information and data collection safely from a remote area.
- The globalizing infocommunication environment has more and more important impact on the methods of technical nature information gathering and on intelligence and law enforcement agencies. According the Global Trends[34] publication of US National Intelligence Council, *„the widespread use of new communications technologies will become a double-edged sword for governance."* and the *„technologies will provide governments - both authoritarian and democratic - an unprecedented ability to monitor their citizens."*

REFERENCES

1. Andrew Griffin: Snoopers' Charter: Theresa May to push huge new spying powers through Parliament, despite major report concluding they are not needed, 11 June 2015 http://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-theresa-may-to-push-huge-new-spying-powers-through-parliament-despite-major-report-10313042.html
2. Boda J. - Dobák I.: A technikai-műszaki nemzetbiztonsági szolgálatok és feladatok jelentősége a 21. században, In: Boda József, Dobák Imre (ed.) A nemzetbiztonság technikai kihívásai a 21. században, Bp., NKE Szolgáltató Nonprofit Kft, 2015.
3. Council Resolution, of 17 January 1995 on the lawful interception of telecommunications (96/C 329/01), Official Journal of the European Communities C 329, 4.11.1996. Volume 39, ISSN 0378-6986 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:1996:329:FULL&from=EN

[34] Global Trends 2030, ALTERNATIVE WORLDS, NIC 2012-001, ISBN 978-1-929667-21-5.p.7. available at: https://globaltrends2030.files.wordpress.com/2012/11/global-trends-2030-november2012.pdf (access: August 15, 2017)

4. Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében, Hadmérnök XII/2, 2017. p. 236, http://hadmernok.hu/172_19_dobak.pdf
5. Don’t Panic, Making Progress on the “Going Dark”, Debate February 1, 2016, The Berkman Center for Internet and Society at Harvard University, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf
6. Global Trends 2030, Alternative Worlds, NIC 2012-001, ISBN 978-1-929667-21-5. https://globaltrends2030.files.wordpress.com/2012/11/global-trends-2030-november2012.pdf
7. Glyn Moody, 2/3/2016, Revised Snooper’s Charter ignores key criticisms, widens police powers further, http://arstechnica.co.uk/tech-policy/2016/03/revised-snoopers-charter-ignores-key-criticisms-widens-police-powers-further/
8. Glyn Moody, 17/11/2016, Why the Investigatory Powers Act is a privacy disaster waiting to happen, http://arstechnica.co.uk/tech-policy/2016/11/investigatory-powers-act-privacy-disaster-waiting-to-happen/
9. Glyn Moody, 8/6/2016, IP Bill’s metadata stores “more intrusive” than comms data—top UK cop tells Ars, Virtual single database of citizens written by UK gov't could be recipe for disaster, https://arstechnica.co.uk/tech-policy/2016/06/ipbill-metadata-icr-more-intrusive-than-comms-data-analysis/
10. James B. Comey: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? October 16, 2014 available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf
11. Kris D. S. (2016). Trends and predictions in foreign intelligence surveillance: The FAA and beyond, Journal of National Security Law & Policy, 8(3), 1-42. Retrieved from https://search.proquest.com/docview/1831706283?accountid=42933
12. Mirja Gutheil, Quentin Liger, Aurélie Heetman, James Eager, Max Crawford: Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Study for the LIBE Committee Directorate General for Internal Policies Policí Department C: Citizens’s Rights and Constitutional Affairs, European Union, 2017, http://www.europarl.europa.eu/supporting-analyses
13. Ronald Bailey: Is Russia’s Surveillance State Being Modelled onthe West?, New Russian anti-encryption and data retention laws look sadly familiar. Jul. 22, 2016, reason.com, https://reason.com/archives/2016/07/22/is-russias-surveillance-state-being-mode/print
14. Russia's State Duma just approved some of the most repressive laws in post-Soviet history, Meduza, 16:36, 24 June 2016, https://meduza.io/en/feature/2016/06/24/russia-s-state-duma-just-approved-some-of-the-most-repressive-laws-in-post-soviet-history
15. Susan Morgan: “Lawful Interception and Government Access to User Data: Designing a Rights-Respecting Model” (Jan. 2016). Institute for Human Rights and Business, Occasional Paper Series Paper Number 5, Institute for Human Rights and Business (IHRB), https://www.ihrb.org/uploads/reports/2016-1-15_Lawful_Interception_Government_Access_User_Data.pdf

16. The Guardian, NSA files: Decoded https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1
17. The use of the Internet for terrorist purposes, United Nations Office on Drugs and Crime, Vienna, UN, 09.2012. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
18. UN General Assembly, 16 November 2016 A/C.3/71/L.39/Rev.1, https://www.accessnow.org/cms/assets/uploads/2016/09/privacy-resolution-2016-UNGA.pdf
19. UN General Assembly, A/HRC/35/22, 30 March 2017, Human Rights Council Thirty-fifth session
20. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, p.6. available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement
21. UN Human Rights Council. 2015. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/29/32
22. What is 'safe harbour' and why did the EUCJ just declare it invalid? https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection
23. Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, R. B. J. Walker; After Snowden: Rethinking the Impact of Surveillance, International Political Sociology, Volume 8, Issue 2, 1 June 2014, p. 121–144, https://doi.org/10.1111/ips.12048
24. https://wikileaks.org/-Leaks-.html
25. http://www.etsi.org/technologies-clusters/technologies/lawful-interception
26. https://www.alliedmarketresearch.com/lawful-interception-market