UNIVERSITY OF PUBLIC SERVICE

Doctoral School of Military Sciences

THESIS BOOKLET

Tamás Tóth:

The effects of changes in the ICT environment on the development of information gathering in the 21st century

for the doctoral (Ph.D.) dissertation

Supervisor:
Dr. habil. Imre Dobák

Budapest, 2024.

CONTENT

1. INTRODUCTION

Nowadays, the dynamic change of the security environment, the intensive development of technologies, and the continuous increase in the amount of available information require from the information gathering agencies[1] organizations that are able to adapt quickly, both in the organizational and operational areas, with efficient information acquisition and processing capabilities. One can experience the increasingly hybrid, asymmetric nature of individual challenges, risks, and threats, as well as actual conflicts, which now range from open regular military conflicts through information operations, terrorism, organized crime, and political and economic pressure and influence. The tendency of the external security environment to change in a negative direction, as well as the rapid development of digitalization and the technological environment, resulted in the creation of a comprehensive security strategies both at the international and national level.

In order to ensure the normal functioning of the society and national sovereignty, the constitutional task of modern state power arising from the protection and security function is to guarantee the enforcement of mutual security, as well as to contribute to it at the level of its international allies. For the citizens of the Hungarian state, their basic rights are primarily ensured by the national defense and law enforcement sector and, from the point of view of the dissertation, by the national security services, judicial and law enforcement agencies, in justified cases by keeping to legal guarantee rules, for example, secret information collection by authorized organizations and by application of covert means and methods (herein referred to as secret information collection).

The largest share of data and information relevant to the collection of information is currently related to an information and communication technology (hereafter: ICT[2]) device, system, or procedure. Disruptive, i.e. "subversive" technologies such as artificial intelligence, autonomous robotics, IoT[3], VR/AR[4], new-generation communications networks, and space technologies are rapidly gaining ground, which are transforming the security environment at an increased rate. Thus, it is essential to continuously develop and adapt the technical capabilities of information

[1] In the dissertation, "information gathering organizations (agencies)" refers to the range of organizations authorized to collect secret information, to use covert means and to implement them.
[2] Information and Communication Technology
[3] Internet of Things
[4] Virtual Reality/Augmented Reality

gathering organizations in order to manage current and expected security, technological challenges, risks, and dangers.

A few years ago, more and more "chat applications" and mobile applications providing encrypted online communication, i.e. application services[5] according to the Hungarian legal term, appeared, which promised secure communication. Among them, the end-to-end encryption cryptographic procedure (hereinafter: E2EE[6]) has become more and more common. In order to prevent, detect and eliminate illegal activities that have a negative impact on public and national security - such as international organized crime, terrorism, illegal arms trade, state and non-governmental efforts that threaten national sovereignty - the content of the related communication plays a significant role, accompanying - and its metadata for the purpose of national security and law enforcement covert, legal recognition, i.e. legal control (hereinafter: LI [7]).

The primary subject of the scientific investigation of the dissertation is the LI activity of encrypted application services that implement interpersonal online communication within the scope of infocommunication services related to the information society for the purpose of national security, naturally examining the related aspects of electronic communications used as communication channels and other services related to the information society, and also in a kind of comparative manner LI for law enforcement purposes. The main subject of the dissertation research work is the passive, deep packet inspection within the individual LI methods, i.e. DPI (Deep Packet Inspection), its central monitoring subsystem-type form realized on the communication network side, of course also examining the aspects of other LI methods, for example service provider cooperation. It is also justified to examine the regulatory and technological environment of LI, in addition to analyzing changes in the security environment and ICT trends and tendencies within society.

---

[5] In this dissertation, under the application service provider, we refer to the Act No. CVIII of 2001 “on certain issues of electronic commercial services and services related to the information society (hereinafter with Hungarian abbreviation: Ekertv.) within the scope of service providers according to Section 2, point m) shall mean service providers providing encrypted online communication.

[6] End-to-End Encryption: Enables decryption of the encrypted message in an understandable form only on the sending and receiving device, within the same service in terms of applications.

[7] Lawful Interception: Legal "eavesdropping", legal communication monitoring. In the course of the dissertation, a broader concept of LI is applied, i.e. in addition to content control, access to accompanying and metadata related to communication is also included. This kind of interpretation is justified by the development of the ICT environment, since it is also possible to check these on communication networks and information systems.

2. DEFINITION OF THE SCIENTIFIC PROBLEM

In order to take an effective, prognostic approach against persons and groups involved in the activities of the national security services, who may be associated with behavior that violates national sovereignty, terrorism, and other highly dangerous crimes for society, it is essential to maintain LI capabilities that are resistant to social, technological, and normative challenges within the complex tool system of secret information gathering. As a result of the digital market and data protection strategic objectives of the EU, the transformation of the markets for consumer electronic communications and other Internet-based communication services related to the information society is being experienced, so from the point of view of the dissertation, the increasing demand for application services is primarily the increasing demand for application services, which is digitization, virtualization, continuous online can be identified as a priority component in order to satisfy the needs for presence. The "dumping" of demand in connection with disruptive infocommunication products and services caused a kind of supply R+D+I "shock" in the ICT market of the 21st century, as a result of which the increasingly dynamic development of infocommunication technologies and the ICT environment can be seen, including new data transfer solutions, both in terms of more sophisticated electronic information and cyber protection procedures, as well as normative data protection regulations. Based on the justification of the choice of topic, the use of these internet-based, encrypted online communication application services can be identified at a presumably increasing rate in the communication attitude of the persons and groups involved in the activities of the national security services - and law enforcement agencies - which is also a trend according to the rules of market demand/supply in the "LI market". can also presumably result in growth.

Based on the justification of the choice of topic, I identify the challenges arising from the development of the ICT environment and their effects on the efficiency and skill development of the LI as a problem area to be scientifically investigated in terms of the effective monitoring of interpersonal communication on electronic communication networks in Hungary. Based on the literature, it can be established that up to and including 2015-2016, the control of application services at the state level encountered normative and technological difficulties. Based on the justification of the choice of topic, it is necessary to carry out a thorough scientific examination of the topic following this date, during which the sub-topic is primarily the effectiveness of the legal and technological environment of the LI of the application services for domestic national

security, thus its resilience against the development of the ICT environment[8]. In connection with the LI of application services, it is also justified to conduct a scientific examination of electronic mobile (telephone, internet) communication services and their LI, which in most cases provide a communication channel.

From the point of view of the effectiveness of LI, it is also necessary to examine the development of the cryptographic environment of both communication networks and application services. In addition, the examination of the characteristics of the security environment, as well as the ICT habits and trends of society, i.e. the users, is also essential for determining the direction of skill development. It can be concluded that the collection of technical information, interpreted as a sub-activity within it, affects the efficiency of the LI ability directly and indirectly by a number of interrelated, very complex external effects resulting from the continuous change and development of the ICT environment, among which, during the research work, the regulatory, technological, social, and an examination of the security environment is justifiable[9]. During the research work, it is possible to draw scientific conclusions about the additional LI opportunities and challenges arising from the development of the ICT environment, which can be of added value to the ability development aimed at the effectiveness of LI. In order for the LI activity concerning application services to be effective in the future in Hungary, it is essential to draw conclusions from a prognostic point of view:
with regard to the global and domestic trends, trends and evolution of the digital ICT market;

- about LI challenges/additional LI opportunities arising from the development of the ICT market;
- about the domestic organizational system, regulation and evolution of LI activity;
- on the unique characteristics of mobile networks and application services from an LI perspective, and the correlation of activities;
- about the electronic information protection environment of mobile communication networks and application services within the scope of interpersonal information communication services, including the development of cryptographic procedures;
- on the evolution of the normative data protection environment of interpersonal communications;

[8] Resilience: Flexible resistance ability in a general sense, i.e. the reactive ability of a system to successfully adapt against strong, renewable or even shock-like external negative influences.

[9] During the sub-research activities, the effects of the political and economic policy environment, primarily at the EU level, are of course the subject of investigation, but they are mostly enforced indirectly through regulation. Environmental factors will not be examined, given its unreasonableness.

- the evolution of the communication habits of persons and groups involved in the LI activity for application services;
- due to globalized ICT services, about the possibilities of international, EU cooperation of LI for national security and law enforcement purposes.

3. HYPOTHESES

1. Based on the predictable ICT trends, it can be assumed that compared to the traditional LI of GSM-based mobile communication, an increase in the demand for LI of application services providing encrypted online communication based on the mobile Internet is expected, whose LI methods based on service provider cooperation and technical monitoring also create an innovative technological, regulatory and organizational environment are required.

2. In the future, the expected spread of electronic communications networks based on air and space infrastructure, as well as the LI of new generation mobile networks, may revolutionize the technical capabilities of secret information collection with all data sources due to the increasingly heterogeneous nature and source of data traffic, as long as the information collection organizations are able to exploit the opportunities from a technological point of view.

3. The globalization of application services and the development of the international data protection normative and technological environment may adversely affect the effectiveness of the LI of communications carried out on them, and as a result of their cryptographic development, the effectiveness of the effective domestic norm system regulating communication control may be eroded, and the resilience of the LI capability may be limited in this area.

4. It is likely that in the future, for the sake of the effectiveness of the national security LI of communications carried out within the framework of interpersonal communication services - including application services - it will be essential to increase international, especially EU cooperation, taking into account the possibility of developing the capabilities of future LI in addition to the exchange of information, while respecting national sovereignty.

4. RESEARCH OBJECTIVES

I set the main goal to verify the hypotheses, as well as a new scientific result by creating proposals that can promote the future effectiveness of LI. Within the defined general scientific problem area, I primarily examine the effectiveness of the legal and technological environment of the domestic LI of application services, as well as its resilience against the development of cryptographic procedures, and the possibilities of individual LI efficiency-enhancing measures aimed at national security, in accordance with the National Security Strategy of Hungary (hereinafter: Strategy) with its overall objectives, examining the effects of the EU's digital market and data protection strategic objectives regarding the topic. To this end, based on the analysis of the main interpersonal ICT trends and tendencies, I will draw conclusions about the development of the relationship system of traditional mobile communication and mobile Internet-based communication, as well as the relationship system of LI that affects them, based on the analysis of the evolutionary processes of communication and domestic LI activity. I compare the domestic normative environment of LI activity for mobile communications and application services, and then draw conclusions about their effectiveness, examining the additional LI opportunities arising from the development of the ICT environment.

Based on a general examination of the cryptographic environment of both mobile networks and application services, I determine which are the main cryptographic characteristics affecting the subject of the study, as well as what efficiency-limiting characteristics they have in terms of LI. I also draw conclusions regarding the effects of the development of the cryptographic environment and certain global events affecting users' data management attitudes on changes in demand for application services. Analyzing the domestic normative environment of LI of application services for national security purposes, and comparing it with the cryptographic development interpreted in the context of electronic information protection, I draw conclusions about the resilience and effectiveness of communication control.

During the course of the dissertation, my aim is to look at the forms of use of application services for illegal purposes, proving with practical examples the raison d'être of their control, as well as the danger to society of the limited effectiveness of LI. In view of the globalization of electronic communications, in the course of the dissertation I draw conclusions about some international experiences of LI activity, LI-type challenges affecting application services, and I also compare the system of international cooperation aimed at LI for national security and law

enforcement purposes, on the basis of which I evaluate LI for national security purposes the actualities of its international cooperation and the relationship between the two spheres of activity. Furthermore, I provide an international outlook, primarily regarding the challenges and practices related to the LI of application services, as well as the opportunities for international cooperation. I draw conclusions regarding the concrete effects of the change in the ICT environment on the collection of secret information, primarily from the aspect of LI in terms of strategy-making, legislation, and actual LI capabilities. The time frame of the prognostic examination of the dissertation fits the “by 2030” time frame of the EU Digital Decade 2030 policy program and the domestic Strategy 2030.

The main goal of the doctoral dissertation alas the dissertation, based on the scientific conclusions reached during the above analyzes and investigations, is to achieve practice-oriented, public scientific results that can be integrated into applied research, which carry within themselves the possibility of contributing to the improvement of the efficiency of domestic LI capabilities, primarily legislative directions, attitude formation, further sub-research by defining directions. In addition to the systematic overview of the processed literature, the research is primarily intended to reveal new scientifically sound connections and draw conclusions regarding each of the investigated topics. I intend to achieve the objectives by applying the following research and investigation methods, at the same time by creating a new scientific methodology of LI research for the purpose of national security, and by applying it during the dissertation.

5. RESEARCH METHODOLOGY

Statistical data analysis, trend and trend analysis, professional historical research, legal analysis and interpretation, document and content analysis, as well as a complex approach and some quantitative and qualitative analysis of the data and information based on them are used as defining research methods during the dissertation, evaluation, and case study-type processing. During the processing of the literature and the critical review of the sources, I also rely on the comparative analysis method of the analysis work. Reasonableness, the application of logic, thorough and objective "observation" and analysis prevail as basic principles throughout the research work.

In the course of the dissertation, in addition to the processing of the literature related to certain infocommunication trends and tendencies regarding mobile communication services and application services, openly accessible current and predictive statistical data are qualitatively analyzed and evaluated. The question of the reliability and credibility of the available sources and statistical data can be identified as a research challenge, so they are processed widely and compared to each other for the sake of authentic source analysis.

The domestic normative environment of LI for the purpose of national security - and, for comparative purposes, law enforcement - will be the subject of the investigation, with the document and content analysis of relevant literature and legislation, the parallel processing of domestic and international legal sources, including EU legal sources, and EU aspirations related to digitalization. The jurisprudence of the European Court of Human Rights (hereinafter: ECtHR), the Court of the European Union (hereinafter: CJEU) and the Hungarian Constitutional Court will also be presented during the presentation of some of their decisions related to the topic. In addition, some relevant decisions of the European Data Protection Board (hereinafter: EDPB) and the National Data Protection and Freedom of Information Authority will also be processed regarding legal disputes affecting the limitation of the right to self-determination of information.

During the evolutionary investigation of the domestic organizational system and activities of legal communication control affecting communications and application services, the development of domestic technology and regulation in the 21st century is reviewed along the lines of the above criteria, using an integrated, complex methodology, professional history documents, standards and legislation related to LI, as well as by comparing statistical data. In order to provide a practice-oriented approach to the dissertation, international examples and challenges related to the illegal use of application services are processed in the form of case studies.

The research methods of the dissertation do not include technical, technological analysis or measurement. Classified data according to Hungarian Act No. CLV of 2009 on the protection of classified data during the application of research methods will not be processed, managed or disclosed in the dissertation.

The longer-than-average scope of the justification of the choice of topic and the relevance of the research, the formulation of the scientific problem, and the above methodological description made visible the very complex topic requiring scientific investigation, which, based on its components

- has a strict logical structure (progresses from the general and narrows to the specific);
- has an integrated content (professional knowledge of national security and law enforcement; trend analysis; norm analysis; technological and digitization knowledge);
- based on a related activity objective (national security objective, law enforcement objective)

requires a complex research methodology in order to support the hypotheses and realize the objectives of the dissertation. For this reason, I developed the "integrated interdisciplinary scientific methodology of LI research for national security" used during the dissertation research work, which is illustrated in the figure below - number 2 in the dissertation:

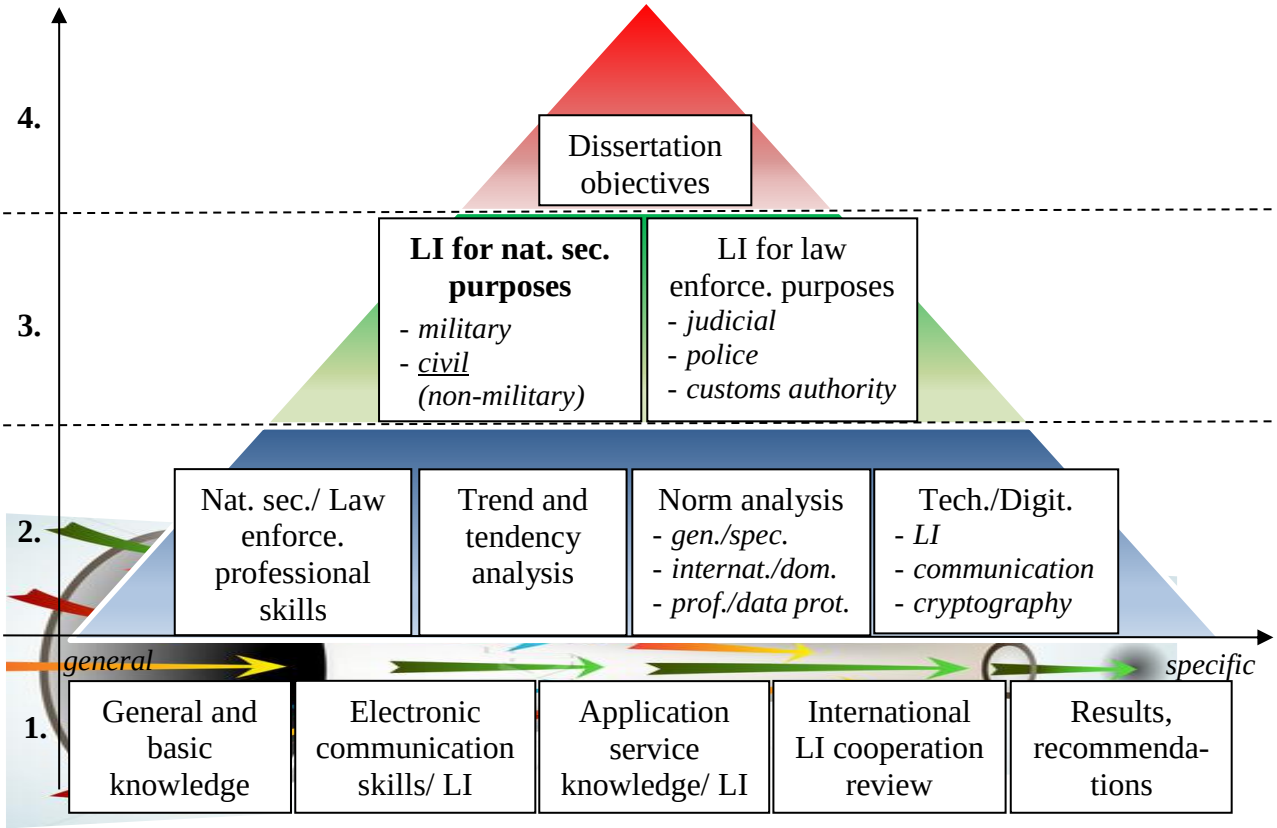

Figure 1: Integrated interdisciplinary scientific methodology of LI research for national security purposes [10]
(Editor: The author)

[10] Abbreviations: Nat. sec./ Law enforce. professional skills – National security and law enforcement professional knowledge; gen./spec. – general and special; internat./dom. – international and domestic; prof./data prot. – professional and data protection; LI for nat. sec. purposes – LI for national security purpose; LI for law enforce. purposes – LI for law enforcement purpose.

In the framework of the dissertation research work, based on the developed research methodology, during the processing of the literature[11], in accordance with the hypotheses, in accordance with the structure of the dissertation [12], the individual content aspects are analyzed in an integrated way in the subsections, along with the goal-based examination of the activity, the main direction of which is the "civilian national security goal"[13]. Thus, vertically completing the dissertation objectives located at the top of the pyramid, and horizontally achieving new scientific results, formulating recommendations, and finally completing the doctoral (PhD) dissertation.

6. BRIEF DESCRIPTION OF THE EXAMINATIONS PERFORMED CHAPTER BY CHAPTER

The dissertation is divided into 11 main chapters, at the end of each chapter the partial conclusions are drawn that can be established based on the research activities of each subsection. In the introductory part of the dissertation, i.e. chapter 1, the rationale for choosing the topic and the topicality of the research, the formulation of the scientific problem, the hypotheses, the purpose of the dissertation, the research methodology, the overview of the literature, and the structure of the dissertation, its structure, and presentation of the main content of further subsections.

The main content of the first part of the dissertation, i.e. chapter 2, is an overview of the warranty, organizational, conceptual and methodological background of LI as a kind of introduction, as a discussion of the necessary basic knowledge, in order to prepare the research actions included in the following chapters. Within the chapter, the content of the "national security goal" is interpreted in a total of 7 sub-chapters as a preliminary question, the international and domestic framework of LI regulation, an overview of the basic legal and data protection guarantee background of LI, and then an analysis of the effects of the EU's digital market and data protection strategic objectives on LI are the subject of investigation. aspect. The description of LI's domestic organizational system and its general normative background,

[11] See: “1.6. Literature review" subchapter of the dissertation.
[12] See: “1.7. The structure of the dissertation” subchapter of the dissertation.
[13] See: Hungarian Act No. CXXV of 1995 on the national security services (hereinafter with Hungarian abbreviation: Nbtv.) § 2 (1) para. purpose of the activities of civil national security services (Information Office, Constitutional Protection Office, Special Service for National Security – hereinafter: SSNS, National Information Center).

its information theory background and its transfer to the normative environment, some of its main methods and procedures, the necessary basic knowledge of cryptography and an overview of its challenges are also interpreted.

The main content of the second part of the dissertation, i.e. chapter 3, is the complex and systematic analysis of ICT trends and tendencies related to mobile communication control based on the defined research methodology, in order to support the hypotheses and carry out the sub-research work necessary to achieve new scientific results. The evolution and development trends of electronic digital mobile communication networks, the user trends of mobile networks, the evolution and trends of the cryptographic environment of mobile networks, with a view to LI standardization, and the normative, organizational and technological evolution and trends of domestic telecommunications communication control are the subjects of investigation in a total of 3 sub-chapters. The main content of the third part of the dissertation, i.e. chapter 4, is the complex and systematic analysis of ICT trends and tendencies affecting the LI of application services based on the defined research methodology, in order to support the hypotheses and carry out the sub-research work necessary to achieve new scientific results. Within the chapter, in a total of 4 sub-chapters, the user trends of application services, data protection trends related to application services, security challenge trends and response measures in the international space, and the effective domestic normative and organizational evolution and trends of LI of application services are the subject of investigation.

The final part of the dissertation, which serves to draw and summarize the conclusions, is chapter 5, in which the complex effects of the ICT environment change on the strategic, legislative and LI capabilities concerning the collection of secret information, the results summarizing the partial conclusions of the chapters along the hypotheses are presented. In chapter 6, the dissertation research results recommended for acceptance as new scientific results are listed item by item. Chapter 7 contains specific recommendations and suggestions for the practical use of the research results. Finally, in chapter 8, the preparation of the dissertation, the list of literature used during the dissertation research work, in chapter 9, the list of figures, in chapter 10, the list of publications, and then in chapter 11, the list of appendices and their attachments are presented.

7. SUMMARY AND CONCLUSIONS

After justifying the topic of the dissertation and the actuality of the research, formulating the scientific problems related to it, based on the "integrated interdisciplinary scientific methodology of LI research for national security" determined in accordance with the objectives of the research along the lines of the identified hypotheses, after processing the specialized literature, according to the defined structure of the dissertation, the following were realized: some research actions, as well as concise descriptions of the performed tests in accordance with the chapters, together with the deduction of partial conclusions. During the dissertation, the subject of a comprehensive examination was the overview of LI's guarantee, organizational system and methodological background, as a kind of guide, as a complex discussion of the necessary basic knowledge, in order to establish and prepare the examination of further substantive professional parts. After that, a complex analysis of the ICT trends affecting the mobile communication LI and the ICT trends affecting the application service LI related to the information society was carried out based on the defined research methodology, in order to verify the hypotheses. The summary and description of the partial research results of the dissertation regarding the effects of the changes in the ICT environment on the development of information gathering in the 21st century is contained in the following:

Hypothesis 1 was proven, according to which, based on predictable ICT trends, compared to the traditional LI of GSM-based interpersonal mobile communication, an increase in the demand for LI of application services providing encrypted online communication based on the mobile Internet is expected, whose LI methods based on service provider cooperation and technical monitoring are also innovative technological, they require a regulatory and organizational environment. The research actions of each subsection support the hypothesis as follows:

- Section 3.1.; 3.2.; 4.3. based on the research actions of subsections in the field of mobile communication technologies approx. Every 10 years, a generational change is experienced, which is induced by the continuous heterogenization of network traffic, the needs of residential consumers, and the service of new ICT services. Using a trend analysis research method, it was established that on a global level approx. By 2030, 5G residential mobile subscriptions will take the leading role over 4G, almost completely displacing previous technologies (2G, 3G). Overall, the number of mobile subscriptions shows a constantly

rising trend at the global level, so in addition to network modernization, increasing demand can be established, and a correlation between these trends can be identified due to the additional service possibilities of new generation networks. During a trend analysis, it was established that the domestic spread of new-generation mobile networks (4G, 5G) shows the same trend as global and regional trends, i.e. it has a displacing effect on previous technologies. Examining the regional 5G trends, however, it can be concluded that in 2023 Hungary surpassed the Central and Eastern European average. Based on the market trends of application services until 2030-2031, the further growth of their central role in serving the communication needs of the public has been proven, increasing the economic volume of the global market by about 1.7 times between 2029 and 2031, based on the forecasts. In Europe, according to forecasts, the market leaders will continue to be Meta's services (WhatsApp, Messenger), iMessage, Telegram, Signal and Viber.

- Section 2.4; 3.2.; 3.3.; 4.1.; 4.3.; 4.4. based on subsections, during the trend analysis of Meta's attitude towards official data provision, an exponential increase in the global number of official requests received by the service provider is established, which shows the same trend as the expansion of the concept of mobile internet. It can be proven that application services that provide Internet-based encrypted communication are increasingly involved in activities that violate the interests of law enforcement and national security. As a result of increasing personal data protection regulations and demand, the development of E2EE, which significantly limits the effectiveness of the cryptographic properties of application services, primarily the technical LI method of central DPI monitoring, also illegal activities such as terrorism, organized crime, extremism, etc. based on the processed case studies. also provides a conspiratorial opportunity for him. Based on my point of view, there is currently no effective EU legal instrument for the purpose of law enforcement, neither at the level of the member states nor when examining the EU, and multilateral cooperation for national security purposes is based on the cooperation of global application providers (Meta, Apple) with the parent company in the USA and, for example, EU distribution headquarters in Ireland (Meta, Apple) in terms of cooperation-based LI.

- Section 2.5; 3.3.; 4.4. on the basis of subsections, the legislator has now designated the SSNS as the domestic central LI service organization, which provides services to the ordering national security, law enforcement, and judicial agencies, for the implementation of both LI for domestic national security and law enforcement purposes, and international

LI cooperation for law enforcement purposes with its special secret information gathering tools and methods. Compared with the research results of 2015-2016, at that time the LI was more decentralized, at that time it had not yet acquired its present-day centralized form, concentrated in one organization, which includes uniformity in law enforcement, resource optimization, concentrated R+D+I responsibility, and independent organizational also provides internal control. The 2.5. In the subsection, it was revealed that the collection of secret information for national security purposes, which is subject to the permission of the Minister of Justice and the judge, and thus the number of LI shows an average, flat exponentially increasing trend, according to the forecasts, the dominance of national security cases can be predicted. Current skill development efforts are supported by the creation of TIF, InfoLab, MiLab scientific research and development formations.

- The 2.5.3. based on sub-chapter, the traditional systematic classification of LI during the unique handling of application service cryptography challenges implemented in the framework of the "Trojan Shield" action carried out by the international law enforcement coalition led by the FBI with the distribution of the ANOM application service (NI-ICS) labeled as "uninterceptable" in organized criminal circles and conspired to control it its technical assurance was supplemented by the new, innovative "false flag" LI method.

Hypothesis 2 was supported, according to which in the future the expected spread of electronic communications networks based on air and space infrastructure, as well as the LI of new generation mobile networks, may revolutionize the technical capabilities of secret information collection with all data sources due to data traffic of an increasingly heterogeneous nature and source, if the information collection organizations are able exploit the possibilities from a technological point of view, for example in the context of the "Integrated Smart LI" (dissertation: ISLI) concept developed in theory during the research work. The research actions of each subsection support the hypothesis as follows:

- Section 2.5; 3.1.; 3.2.; 3.3.4.; 4.4. during the actions of subsections, the trend analysis research method was used to establish the shift of the national-state character of electronic communication services in the global, but primarily European context, towards the regional, globalizing character, which is supported by the 6G-based, AI-supported, integrated VHetNet electronic communication concept. Thus, it is justified and necessary to take into account the regional prognostic forecasts in terms of the R+D+I of the domestic

LI and the legislation, which in the coming 6-year period in the Central-Eastern European region regarding personal communication for public purposes is therefore justified and necessary. The leading role of 4G is projected, in addition to the exponential strengthening of 5G and the gradual displacement of 4G. Based on the target system of its Space Strategy until 2030, Hungary intends to play a strong role in the development of the space industry and in the domestic distribution of its innovative services, for example in the field of communications, which already justifies such research and the preparation of developments aimed at ensuring LI capability.

- Section 2.7; 3.1.; 3.2.; 3.3.; 4.4. based on the sub-research results of subsections, in the future, 5G and 6G electronic communication networks will contain extremely large amounts of very heterogeneous types of data, for example with regard to certain services of the complex digital ecosystem of the smart city, which are all activities against terrorism, illegal migration, and transnational organized crime can create added value for national security and law enforcement LI. As an optimal strategic research and development direction, 3.3.2. I recommend the development of LI capability according to the ISLI concept presented and proven in subchapter.

- In case of the spread of the 6G-based VHetNet satellite communication infrastructure around 2030/2040 according to forecasts, at least in the framework of international cooperation at the EU level, ISLI 2.0, which respects national sovereignty. I recommend investigating the possibility of LI capability according to the concept. As for ISLI 2.0, in connection with the possibility of this capability, the nature of national security activity as an exception to supranational EU law arises, and the cryptographic environment of individual application services strongly influences the effectiveness of the concept, so further examination of the issue is warranted. In the 4.4.3. sub-chapter proposed LI model for law enforcement and national security purposes, based on service provider cooperation, in my opinion, can be automated in accordance with the expectations of the age, and can be converted into a technical LI method realized through electronic data connection within the framework of the ISLI model. However, the ISLI concept can only ensure full efficiency if, in the case of E2EE suppression, it is possible to create an internationally standardized cryptographic procedure that simultaneously ensures the effectiveness of LI together with the appropriate level of data protection, thus ensuring the balanced enforcement of the value duality of data protection/security.

Hypothesis 3 has been confirmed, according to which the globalization of application services and the development of the international data protection normative and technological environment may adversely affect the effectiveness of the LI of communications carried out on them, and as a result of their cryptographic development, the effectiveness of the effective domestic norm system regulating communication control may be eroded, and in this regard, the LI ability resilience may be limited. The research actions of each subsection support the hypothesis as follows:

- Section 2.7; 4.2.; 4.3.; 4.3.; 4.4. Based on the research actions of subsections, major market-leading application providers, such as Meta, continuously improve the cryptographic properties of applications to make user communication more secure, as well as for marketing purposes, which on the one hand led to the development of protocols and algorithms, and on the other hand to the general spread of E2EE applications, a kind of demand/supply as a self-exciting phenomenon. After the 2014-2016 period, nowadays an "encryption competition" is once again starting to develop on the market of application services, already reacting in advance to the quantum computing-based innovation of the development of the ICT environment. The challenge of anonymity related to application services was presented, for which reason, based on my proposal, it should be established as a requirement for application providers at the global, but at least EU level, to provide the user's mobile phone number during the registration of a natural person for identification purposes. Thus, the authorized law enforcement agencies, even indirectly within the framework of LI for national security purposes, but in the domestic context, the Eht.[14] based on its underlying rules, they could already identify the real user affected by LI much more effectively.

- Section 2.5; 2.7.; 3.1.; 3.3.; 4.2.; 4.3.; 4.4. according to the research actions carried out in subsections, the pioneering Ekertv. 3/B. and 13/B. A conclusion can be drawn in relation to the timeliness of the LI regulation for service providers based on service provider cooperation according to § 2.4.1. on the basis of subchapter, it was already limitedly effective at the time of its entry into force - since the principle of technology neutrality had to prevail - given that ¾ of the examined application services already used E2EE by then. Looking at the actuality of the effectiveness of the provisions, it can be concluded that it is

[14] Hungarian Act No. C of 2003 on electronic communications. (hereinafter with Hungarian abbreviation: Eht.)

further limited by the continuous spread of E2EE's default and, more recently, by the emergence of cryptography that is also resistant to quantum computing.

- The 2.4. and 4.3. on the basis of the partial researches of the subsection, it was established that the EU digitalization strategic objectives resulting from the development of the ICT environment follow a coherent, consistent legal and policy effort in order to strengthen normative and technological information security aimed at enhancing user data protection and trust, thus promoting digital, ICT products and services its spread primarily for economic and social political reasons. However, the comparative volume analysis of the global markets of application services and LI shades the above finding that the volume of the LI market by 2030 will be approx. It will account for 4-5% of the global application services market. Thus, the lobbying activities of market-leading "flagships" with higher technological (mainly cryptographic) R+D+I investment resources cannot be ruled out, in order to establish a marketing-like basis for the increasing user data protection needs and to tighten regulations, thus increasing their market share, expansion, and ultimately in line with their profits, along with displacing competitors, but this is more of a conclusion raising competition law issues. And the marketing-like superiority can be negative in terms of security in that the applications advertise in their information regarding E2EE that the users' communication data is "safe" even in front of the service provider due to the strong cryptography - thus inferring from this the governmental, national security, law enforcement before bodies and authorities.

Hypothesis 4 has been proven, according to which in the future, in order to improve the efficiency of LI of communication for national security purposes within the framework of interpersonal communication services, including application services, it will be essential to increase international and EU cooperation, taking into account the possibility of developing the capabilities of future LI in addition to the exchange of information while respecting national sovereignty. The research actions of each subsection support the hypothesis as follows:

- Section 2.1.; 2.3; 3.1.; 3.3.; 4.3. based on the research actions of the sub-chapters, the international outlook, and the examination of cooperation, in contrast to the inter-member cooperation aimed at LI for the purpose of law enforcement on the territory of the European Union, based on the public literature, in relation to LI for the purpose of national security, there is still no organized effort to develop a normative framework for even partial

multilateral cooperation. However, based on my point of view, activities for the purpose of national security, secret information gathering, including LI, have aspects that can lead to a breach of the regulations, which have a positive effect on the sovereignty and security of the member states cooperating with each other. Such is the activity aimed at national security - but can also be interpreted in the scope of law enforcement interests - for example, as defined by the Nbtv. subsection ae) of § 74. on cooperation by a given national security service in the prevention, detection, prevention and suppression of terrorism, transnational organized crime, for example, trafficking in arms, drugs, human beings and artefacts, as defined in the national security interest. Furthermore, this category includes illegal migration, activities of non-governmental organizations, furthermore third states interfering in the sovereignty of allied states, and crimes against humanity.

- According to the results of the complex sub-research of the dissertation, the communication LI activity is already in connection with 5G, but actually the air and space communication infrastructures of VHetNet, which appear in connection with 6G, due to their location alone, will raise the collision of the jurisdictions of the member states at the EU level, which from the GDPR data protection point of view already prognostically tried to handle it. The conflict of the applicable laws of the Member States will also occur in the field of LI regulation and implementation. Thus, higher framework legislation at the EU level is essential in order to develop effective LI capabilities of the future, for example according to the ISLI model proposed in subsection 3.3.2. From the point of view of successful LI activities in the future, formal international cooperation with legal binding force and effective enforceability is essential in order to judge the law-abiding behavior of global application providers in the field of LI, also bringing EU legislation with it, in cooperation with the USA, for example 4.4.3. according to the LI regulatory framework based on international service provider cooperation for the purpose of law enforcement and national security proposed in the subchapter, which can be converted based on its principle model into the technical LI method of DPI monitoring that can be integrated into ISLI. The degree of effectiveness of the proposed LI models largely depends on the normative measures limiting E2EE, in addition to which, however, personal data protection efforts can prevail, keeping the data protection/security value duality in balance, but still eliminating the already existing "ICT LI data protection security deficit".

As a further meaningful result of the research work, it was revealed and proven that the international and EU data protection efforts and market demands adversely affect the effectiveness of the LI activity by examining the value duality of data protection/security, causing a kind of "ICT data protection security deficit" to the disadvantage of security, and some global ICT service providers abusing them have established a kind of debatably legitimate quasi-legality control, in the framework of which they institutionally refuse a high percentage of requests for data provision based on the national legal order of LI-entitled organizations. The 3.3.; 4.3.; 4.4. the research actions of subsections support the above research result as follows:

- In the course of the research work, the "**ICT data protection security deficit**" theory was identified and supported, a theory in which data protection prevails to the disadvantage of security against the dual value balance of data protection/security. The 3.3.; 4.3.; 4.4. subsection-based research actions, the increasing EU data protection regulations and the strengthening of cryptography adversely affect/will affect the effectiveness of LI, thus the enforcement of the constitutional public interests of national and public security. The reason for this is that the EU formulates enhanced data protection requirements for ICT products and services in order to strengthen user confidence, promote additional consumption, and ultimately economic growth. However, if, due to the limitation of LI for national security or law enforcement purposes, the effectiveness of the system of instruments aimed at enforcing the public interest related to security of the individual member states, and therefore of the EU as a whole, is ultimately indirectly damaged, then complex security is reduced at the level of society as a whole. All of this can adversely affect economic growth efforts, such as the EU's policy and strategic goal of creating a general digital ecosystem, a digital society, through the efficiency of businesses and the decline in consumption. Therefore, "over-encryption" by E2EE may directly harm the interests of national security and law enforcement due to the limitation of the control efficiency of the communication of target persons affected by LI, the importance of which is also indicated by the action of the UN High Commissioner for Human Rights. The CSAM debate also shows the imbalance of the balanced duality of data protection/security towards data protection. The CSAM debate carries a potential opportunity to forge unity at the level of the EU's political leadership, at the same time with an unprecedented momentum, which means the restriction of E2EE for public safety and law enforcement purposes, thus opening the possibility to reverse the "ICT data protection security deficit" in favor of security.

- The highly debatable quasi-legitimate "**legality control**" of cooperation-based official data provision requests by global application providers and the 10-year-old practice of restricting performance, which also prevails during LI for the purposes of national security and law enforcement, thus directly infringing the interest of national security and law enforcement, have been identified and proven. During the 4.3.; 4.4. subsections' research actions, it was established that Meta, within the framework of official cooperation, refused to fulfill ¼ (a quarter) of the directly sent inquiries by the competent authorities of each member state, such as LI organizations, in the framework of a kind of, in my opinion, debatably legitimate service provider "legality control". This "institutionalized" practice violates the sovereignty and security interests of individual democratic states, since state coercion is legitimate and unconditional in the exercise of public power under constitutional guarantees, separation of powers, and checks and balances. Based on the above, formal international cooperation with legal binding force and effective enforceability is essential from the point of view of successful LI activities in the future in order to assess the law-abiding behavior of global application providers in the field of LI, based on my point of view, the field of which should be the EU in terms of European countries, bringing EU legislation with it, in cooperation with US government bodies and ICT service providers.

Other key conclusions and findings:

During the evolutionary analysis of the national security strategy, it became visible that the content of the "national security interest", thus the "national security goal" that can be abstracted from it, changes dynamically, according to the expectations of the age, digital challenges, or R+D+I. It was established and proven that during the etymological and substantive interpretation of EU law in domestic legal sources, the application of the concept of "national security" is not uniform or consistent, the concepts of "national security" and "state security" are blurred, which can be identified as a challenge during the application of norms. Furthermore, 2.3.2. in subsection Infotv. based on the interpretation of the national security and law enforcement objective from a data management point of view.

Ekertv was discovered and proven. application service according to the material scope of the Eht. its correlation with NI-ICS according to its material scope is Ekertv. and based on the Eht., DMA, European Electronic Communications Code, or due to their functional identity, the Ekertv. and the Eht. collision, conflict of its objective scope. A 2.4., 2.6.; 3.3.; 4.4. in

subsections, the above was established during the research actions. The integrated EU legal and policy approach to the regulation of infocommunication and electronic communications services related to the information society finally became essentially a provision of effective and applicable EU law by 2023 during the culmination of the DMA and the Communications Code. Thus, embodying the obligations of legislators and law enforcers at the EU and Member State level, for the first time in the scope of application services within the framework of the European Commission's institutional jurisprudence valid from the end of 2023 with regard to basic platform services (NI-ICS/application service) according to WhatsApp, Messenger and iMessage DMA. In line with the EU's digitization efforts, the digital sector has emerged on the basis of the scope of the DMA and DSA, which has become entrenched and has a significant impact on both the electronic communications and cyber security sectors and regulation (NIS2), the sharp demarcation of legal areas of which, even at the level of the Union, is an emerging process, let alone at the level of member state law. The regulation of NI-ICS/application services is a cardinal issue from the point of view of LI, since the DMA - and already the Telecommunications Code - with regard to NI-ICS extends into the electronic communications sector regulation, which was adopted and transposed in the Eht. at the level of domestic legal sources, so by the way Ekertv. and its material scope continues to cover the application service, the identification of which legal conflict is also a proposed new scientific result from my point of view.

The expected main challenges of the ICT boom of the 21st century, the development of the ICT environment related to application services, threatening the priority interests of national security, such as the increase in the possibility of information communication user anonymity; the danger of limiting the official cooperation of global service providers exercising the status of "standing above" state, EU and international law; the further spread of the use of application services that integrate E2EE online communication among those involved in the collection of secret information; as well as the generalization of E2EE in communication services and the development of further innovative cryptographic procedures.

Based on the summarized conclusions, the main objectives of the doctoral dissertation were fulfilled by applying the new "*integrated interdisciplinary scientific methodology of LI research for national security purposes*" through the verification of hypotheses on the effects of changes in the ICT environment on the development of information gathering in the 21st century, as well as through additional research results. Based on the scientific conclusions

reached during the analyzes and investigations carried out in the framework of the methodology, new proposed scientific results that are practice-oriented, can be integrated into applied research, and are public, and will be exhaustively listed in the next chapter, have been achieved, which carry the actual possibility of contributing to the improvement of the efficiency of domestic LI capabilities, primarily by defining legislative and research-development directions, attitude formation, and further sub-research directions. Giving a kind of framework to the dissertation, as a final justification for the choice of topic and the topicality of the research, I quote point 3 of the general justification of the December 22, 2023 amendment to the Basic Law (Constitution), according to which the Basic Law is intended to promote the application of new scientific and technical results and digital administration at the state level and "*behind the addition of Article XXVI. [...] is the recognition that the development of information and communication technologies [ICT] brings with it a radical transformation of our lives*."

8. NEW SCIENTIFIC RESULTS

During my dissertation research work, I recommend accepting the following as new scientific results developed in the dissertation:

1. I proved that based on predictable ICT trends, in contrast to the traditional LI of GSM-based interpersonal mobile communication, an increase in the demand for LI of application services that provide encrypted online communication based on the mobile Internet is expected, whose LI methods based on service provider cooperation and technical monitoring are also innovative technological, regulatory and organizational they require an environment. **[Proof: 2.4.; 2.6.; 3.1.; 3.2.; 3.3.; 4.1.; 4.3.; 4.4.]**

2. I argued that in the future, the expected spread of electronic communication networks based on aerial and space infrastructure, as well as the LI of new generation mobile networks, could revolutionize the technical capabilities of secret information collection with all data sources due to the increasingly heterogeneous nature and source of data traffic, if the information gathering organizations are able to exploit it from a technological point of view the possibilities, for example, in the framework of the "Integrated Smart LI" (in the dissertation: ISLI) concept developed in theory during the research work. **[Proof: 2.5.; 2.7.; 3.1.; 3.2.; 3.3; 4.4]**

3. I proved that the globalization of application services and the development of the international data protection normative and technological environment adversely affect the effectiveness of the LI of communications carried out on them, and as a result of their cryptographic development, the effectiveness of the effective domestic norm system regulating communication control is eroded, in this area the resilience of the ability to LI is limited. **[Proof: 2.4.; 2.5.; 2.7.; 3.1.; 3.3.; 4.2.; 4.3.; 4.3.; 4.4.]**

4. I have proved that in the future, in order to improve the efficiency of the national security LI of communications carried out within the framework of interpersonal communication services - including application services - it will be essential to increase international EU cooperation, taking into account the possibility of developing the capabilities of future LI in addition to the exchange of information, while respecting national sovereignty. **[Proof: 2.1.; 2.3.; 2.4.; 2.6.3.; 3.1.; 3.2.; 3.3.; 4.1.; 4.2.; 4.3.; 4.4.]**

5. I revealed and proved that the international and EU data protection efforts and market demands adversely affect the effectiveness of LI activities by examining the value duality of data protection/security, creating a kind of "ICT data protection security deficit" to the detriment of security, and some global ICT service providers abusing them and they have created a kind of debatably legitimate quasi-legality control, in the framework of which a high percentage of requests for data provision based on the national legal order of LI-authorized organizations are denied in an institutionalized manner. **[Proof: 3.3.; 4.3.; 4.4.]**

9. RECOMMENDATIONS, PRACTICAL USABILITY OF RESEARCH RESULTS

The practical applicability of the results achieved during the dissertation research work is one of the main objectives of the dissertation in order to generate an actual positive social impact. The results and conclusions - based on my point of view - can constitute a real added value for the complex security ecosystem, so I recommend their practical use according to the recommendations below, both domestic and EU, international legislation, R+D+I according to the national security industrial Triple Helix model for industry, academic and university as well as market players, as well as during higher and doctoral training.

Domestic, EU and international legislation:

I recommend the results related to the proof of the 2nd hypothesis, as well as the Eht. and Ekertv. the use of findings related to the conflict of the scope of the communication and online platform legislation. I recommend 1.-4. results related to hypotheses, as well as the different domestic interpretations of the concept of "national security" appearing in international legal sources, as well as the utilization of findings related to the debatably legitimate "legality control" of official data requests by application providers during the legislation related to the collection of secret information for national security and law enforcement purposes, and to LI. I recommend examining the findings related to hypothesis 3 during the legislation related to personal data protection. In the framework of EU legislation against the sexual exploitation of children, I recommend the 3.-4. the use of the results of hypotheses, which can be more relevant in a domestic context, and the increased validity of the Hungarian position can be further facilitated by Hungary's consecutive presidency of the EU Council in the second half of 2024.

Sectorial national security industrial R+D+I:

I recommend the utilization of the results revealed in 1-4. during the hypothesis proofing and investigation in the theoretical researches of national security, as well as the LI practical research and development, in the investigation of dual use possibilities. I recommend these results to the attention of the InfoLab (National Laboratory of Infocommunication and Information Technology) and MiLab (National Laboratory of Artificial Intelligence) operating under the supervision of the National Office of Research, Development and Innovation, as well as applied research within the framework of the Innovation and Research Center of Military National Security Service. Furthermore, for civil national security scientific work and basic research in the framework of TIF (Science and Innovation Forum).

Academic and university national security industrial R+D+I:

I recommend Hungarian Research Network to 1-3. the utilization of the results achieved in the context of the investigation of hypotheses in the course of research on communication and online platforms. I recommend to the attention of the University of Public Service of Hungary (hereinafter: NKE) the use of walls related to hypotheses 1 and 3 for the purpose of formal doctoral research in military and police science, including national security. I also recommend the utilization of hypotheses 1 and 3 to the attention of the BME Budapest University of Technology and Economics (hereinafter: BME), especially for the applied research related to cryptography and cyber defense taking place within the framework of CrysyLab. I recommend

considering the 1st and 4th hypotheses and the different national interpretations of the concept of "national security" during the doctoral and higher education programs of the Pázmány Péter Catholic University (hereinafter: PPKE) and the University of Pécs (hereinafter: PTE), as well as the jurisprudential utilization of the findings related to the "legality control" of application service providers, even for the purpose of determining new research directions.

Marketing national security industry R+D+I:

I recommend 1.-4. the utilization of the results and findings discovered during the examination of hypotheses in research areas such as AI, autonomous systems and disruptive ICT technologies, primarily for the technical support of industrial R+D, as well as for the contribution to national innovation platforms. I recommend using the results in the development of dual-use products and services of future defense capabilities, thus the complex defense innovation ecosystem, by exploiting the in-depth expertise available in our country and in the region. I recommend the utilization of the results, for example in the framework of dual-use R+D projects dealing with European information operations, with the aim of increasing the common security of the EU member states and increasing the integration and efficiency of the European defense market.

Education and training:

I recommend taking into account the general utilization of the conclusions and research results of the dissertation for the NKE during the theoretical education of national security, for the BME during the training related to the practical connections of cyber defense and national security technologies, and for the PPKE, PTE during the national security and telecommunications law training. Furthermore, in case of actuality, timeliness, and necessity, I recommend the educational and communication use of scientifically based educational and communication support for the high level of compliance with the guarantee conditions of the state of law for LI activity aimed at national security.

10. PUBLICATION LIST OF THE CANDIDATE SUBMITTED IN THE TOPIC

1. DOBÁK, Imre – TÓTH, Tamás (2023). A külső környezet és tendenciák nyomon követésének szükségessége a stratégiaalkotás tükrében. In DOBÁK, Imre – RESPERGER, István (ed.): *Stratégiák, stratégiai gondolkodás, nemzetbiztonság*. Budapest: Ludovika Egyetemi Kiadó. 33–50. ISBN: 978-963-531-85-1-3

2. TÓTH, Tamás (2023): Actualities of certain security aspects of cryptography with regard to information societies. *National Security Review*, 9(1), 107-118. ISSN 2416-3732
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2023_1_NSR.pdf#page=107

3. TÓTH, Tamás (2022): Magyarország Nemzeti Biztonsági Stratégiájának nemzetbiztonsági aspektusú elemzése. *Szakmai Szemle*, 20(3), 69-99. ISSN 1785-1181
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_3_szam.pdf

4. TÓTH, Tamás (2022): Az információgyűjtés új típusú kihívásai a mobil hírközlési hálózatok technológiai fejlődésének aspektusából. In SZELEI, Ildikó (ed.): *A hadtudomány aktuális kérdései napjainkban II*. Budapest: Ludovika Egyetemi Kiadó. 105-122. ISBN: 978-963-531-61-6-8
   Online: https://webshop.ludovika.hu/termek/konyvek/hadtudomany/a-hadtudomany-aktualis-kerdesei-napjainkban-ii/

5. TÓTH, Tamás (2022): Magyarország nemzeti biztonsági stratégiai evolúciója, annak aktualitásai és főbb nemzetbiztonsági vetületei. *Szakmai Szemle*, 20(2), 58-73. ISSN 1785-1181
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_szam.pdf#page=58.

6. DOBÁK, Imre – TÓTH, Tamás (2022): Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle*, 69(2), 195-212. ISSN 2677-1632
   Online: https://ojs.mtak.hu/index.php/belugyiszemle/article/view/5345/4209

7. TÓTH, Tamás (2020): A mobilhálózatok technológiai fejlődéstörténete: Az analóg hangátviteltől az 5G-hálózatokig. *Nemzetbiztonsági Szemle*, 7(4), 44-60. ISSN 2064-3756
   Online: https://doi.org/10.1007/s11276-015-1165-z

8. TÓTH, Tamás (2020): Az információgyűjtő szervezetek technikai képességeire ható külső közvetett tényezők. *Felderítő Szemle*, 19(2), 43-57. ISSN 1588-242X
   Online: https://www.knbsz.gov.hu/hu/letoltes/fsz/2020-2.pdf#page=43

9. TÓTH, Tamás (2020): Az egyes social engeneering módszerek elhatárolása és rendszerezése. *Szakmai Szemle*, 18(1), 87-110. ISSN 1785-1181
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2020_1_szam.pdf#page=87

10. TÓTH, Tamás (2020): New challenges of recruiting personnel for the national security services in light of the information society. *Belügyi Szemle*, 68(2 – Special Issue), 125-139. ISSN 2677-1632
Online: http://doi.org/10.38146/BSZ.SPEC.2020.2.9

11. TÓTH, Tamás (2019). A Nemzetbiztonsági Szakszolgálat felvételi eljárási rendszere. *Belügyi Szemle*, 57(1), 53-67. ISSN 2677-1632
Online: http://doi.org/10.38146/BSZ.2019.1.4

12. TÓTH, Tamás (2019): General description of social engineering and its place in information warfare. *National Security Review*, 5(1), 42-55. ISSN 2416-3732
Online: https://doi.org/10.38146/BSZ.SPEC.2020.2.9

13. TÓTH, Tamás (2019): Az Európai Unió tervezett kiberbiztonsági tanúsítási keretrendszerének bemutatása *Szakmai Szemle*, 17(1), 97-115. ISSN 1785-1181
Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2019_1_szam.pdf

14. TÓTH, Tamás (2019): A digitális alapú, integritás centrikus közszolgálati szervezetek személyi integritását sértő tényezőinek kialakulása, valamint kihívásaik az információs társadalom tükrében. *Rendvédelem*, 8(1), 50–132.ISSN 2560-2349
Online:https://epa.oszk.hu/03300/03353/00014/pdf/EPA03353_rendvedelem_2019_1_050-132.pdf

15. TÓTH, Tamás (2018): A NATO Kibervédelmi Kiválósági Központ bemutatása. *Nemzetbiztonsági Szemle*, 6(4), 48–62. ISSN 2064-3756
Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1485/804

16. TÓTH, Tamás (2018): Humán kockázatok a kritikus információs infrastruktúrában. *Rendvédelem,* 7(1), 149–176. ISSN 2560-2349
Online:https://epa.oszk.hu/03300/03353/00012/pdf/EPA03353_rendvedelem_2018_1_150-177.pdf

17. TÓTH, Tamás (2018). Az üzleti információszerzés új kihívásai a szervezett bűnözés XXI. századi paradigmaváltásának következtében. *Szakmai Szemle*, (1), 102–122. ISSN 1785-1181
Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2018_1_szam.pdf

11. PROFESSIONAL-SCIENTIFIC BIOGRAPHY OF THE CANDIDATE

From 2014, Tamás Tóth held different non-commissioned officer, officer and then higher leader's positions initially in the staff of the Pest County Police Headquarters and then the National Security Special Service. In 2015, he obtained a professional qualification as a police non-commissioned officer, then in 2017 a college degree along with a police administration organizer at the NKE Faculty of Law Enforcement, and in 2019 a certified national security expert university degree at the NKE Faculty of Military Sciences and Officer Training. He continued his studies and in 2020 received a specialized management qualification in electronic information security at NKE Institute of Further Education in Public Administration, in 2023 he received a certified cyber security expert university degree from NKE Faculty of Public Governance and International Studies, and in 2024 he is expected to obtain a certified legal university degree from PPKE Faculty Law and Political Sciences. He has a complex intermediate language knowledge of English and Spanish.

He is a member of the National Security Section of the Hungarian Military Science Society, the Civil National Security Section of the Hungarian Society of Law Enforcement, the Information Security Section of the Communications and Information Science Association, performed the duties of secretary of the Artificial Intelligence Working Group of the Academic Council of the Home Affairs, and participated in the work of the NKE National Security College. The State Secretary for Public Administration of the Ministry of the Interior awarded him a certificate of recognition twice in recognition of his works submitted to scientific tenders announced by the Academic Council of the Home Affairs.

He has published a total of 15 peer-reviewed domestic peer-reviewed scientific journal articles on his research topic, of which 3 are in foreign languages. Furthermore, he wrote 2 book chapters and 3 abstracts. He is a regular lecturer at the closed professional and scientific conferences of the civilian national security sphere, and also participated in the XXXIII. at the Military and Law Enforcement Section of the National Scientific Student Conference. In connection with his research topic, he also participates in the activities of the NKE as a lecturer, and in the National Security MSc/BSc courses of the NKE, he also performs the tasks of thesis supervisor and thesis reviewer. He is an active participant in the cooperation between national security and the scientific sphere.