NATIONAL UNIVERSITY
OF PUBLIC SERVICE
Doctoral Council

BRIGADIER GENERAL
ZOLTÁN KOVÁCS

Author's summary and official reviews of PhD dissertation titled

- The National Security Challenges of the Infocommunication Systems -

Budapest
2015

NATIONAL UNIVERSITY OF PUBLIC SERVICE

BRIGADIER GENERAL ZOLTÁN KOVÁCS

Author's summary and official reviews of PhD dissertation titled

- *The National Security Challenges of the Infocommunication Systems* -

Supervisor:

Prof. Dr. Kovács László ezredes (PhD)
professor

Budapest
2015

1. THE DESCRIPTION OF THE SCIENTIFIC PROBLEM

In recent decades, the infocommunication systems have been developing rapidly. The worldwide spread of mobile communication systems and the Internet, the continuous increase of the bandwidth available for data transmission, and the growth of user contingency have resulted a fast and mass data exchange, which have become the part of our life. With the application of widespread technologies we are able to solve both our everyday issues and work tasks in a cheap and fast way. The two recent determinative trends of infocommunication are the advance of cloud computing and the growth of the market share of mobile devices and the applications running on them.

These trends present a **twofold challenge** for the national security services and law enforcement agencies. **On the one hand**, the new technologies **will be employed** by either these bodies or the state leaders who are protected in the terms of information security by them. This is why we have to make sure that these systems meet the usually high security standards, and at the same time we have to be aware of the remaining security risks. **On the other hand, in the case of new technologies the lawful monitoring in their competence shall be done.**

Currently there is not an existing recommendation which determines what criteria have to be or should be examined for a comprehensive security analysis in case of the application of cloud computing at organization level, as there is not a single recommendation which has to be or should be educated to the protected leaders in the framework of an information security awareness training.

Moreover, there is not such comparing analysis supporting the national security services that presents the recent technical methods suitable for the lawful monitoring of the new technologies; compares their advantages and disadvantages, in addition, there is not a unified system of criteria which could examine an existing or a new technical monitoring method in terms of whether it is suitable to a given task or not. Furthermore, it appears as a hiatus that only the traditional telecommunications providers have definitions suitable for laws, the new type or recently appeared providers do not, and it significantly counterworks the efficient lawful monitoring.

2. RESEARCH GOALS

Based on the above, my research has two goals. I examine the services based on Internet-technology, emphasizing cloud computing systems from the modern infocommunication systems, firstly from the users' aspect, secondly from that of the legal monitoring.

From the users' view I have two main objectives. On the one hand, to establish a security requirement framework which could be used for examining the above mentioned systems, primarily cloud computing systems, and the risks of their usage could be measured. On the other hand, to develop the content of a possible security awareness training about the usage of these systems for protected leaders.

In terms of lawful monitoring my goal is to set up a framework to demonstrate the possibilities of the lawful monitoring of the above mentioned systems, with their advantages and disadvantages, risks, and draws up recommendations concerning their installation, as well as it gives definitions for the recently appeared service providers – even integrating in the law.

I wish to accomplish my aims by using and further developing the recommendations established by international organizations or the national organizations of developed countries, the industry's standards and best practices, and the public information available on lawful monitoring, as well as the adjustment of these pieces of information to the needs of the national security and law enforcement agencies. While selecting research fields I concentrate on those subtasks which are not elaborated and appear as unsolved issues for the national security services and law enforcement agencies.

I accomplished my research goals by dividing the research into the following subgoals:

1. establishing the requirement framework for the security examination of cloud computing systems;
2. elaborating on the content of an information security awareness training for protected leaders;
3. establishing the possibilities of lawful monitoring of the services based on Internet technology and their regulations.

3. RESEARCH METHODS

For my dissertation I used the research methods mentioned below:

- literature research: researching, studying and processing the relevant international and national literature, rules of law and other documents;
- comparative analysis;
- generalization as a research method;
- secondary analysis of research papers: analysis and process of previous research results;
- logical analysis: process, analysis and assessment of uncovered data, after conclusion producing recommendations;
- empiric research: utilization and description of the professional experience gained during the research;
- taking part in conferences, consultations, events, projects and working on regulations proposals;
- publication of results: process of the research results, publication of that results in university textbooks, and presentations at conferences and in education.

4. THE BRIEF SUMMARY OF THE RESEARCH BY CHAPTER

Duly to the paragraphs above, I built up my dissertation pursuant to the four chapters below:

In **chapter one** I discuss the interpretation of cloud computing, I examine their features, the advantages and disadvantages classified by service and deployment models. I analyse the differences between cloud computing and virtualization; outsourcing and services based on Internet technology. I examine whether the concept of governmental cloud and law enforcement cloud could be explained today, as well as I present that the national security services and law enforcement agencies have to deal with cloud computing.

In **chapter two** I analyse and evaluate the public and relevant security recommendations established by national and international organizations dealing with cloud computing, and then I set up new criteria which could be applied to the complex examination of the systems mentioned above. By means of this and summarizing and also completing the analysed recommendations, I create a template for the law enforcement agencies, which enables the security analysis in a unified framework.

In **chapter three** I analyse the main issues of the data security training of protected leaders, and I present the necessity of extension of the data security protection of protected leaders to the cyberspace they use. By means of my criteria mentioned in the previous chapter I analyse the features and the risks of the most frequently used services based on Internet technology and the portable infocommunication devices for personal use, then I make a possible method to prepare the protected leaders for the security-awareness usage with the help of a framework of customization for the above mentioned protected leaders.

In **chapter four** I examine the lawful monitoring of services based on Internet technology. Based on international examples gained from open sources I demonstrate what kinds of methods are available for lawful monitoring, and what kinds of technical or legal problems emerge during their application. With their utilization I set up general criteria for the examination of the lawful monitoring methods, by means of which the authorized services can examine the suitability of the current or a new method for the particular tasks. Besides, I propose a new model which can replace the obsolete telecommunication model by giving definitions that could be integrated in law for each parties involved.

5. SUMMARIZED CONCLUSIONS

While writing my dissertation I concentrated on the national security challenges of cloud computing, at the same time I considered the fact that these systems cannot be examined separately.

In chapter one I presented cloud computing, its definitions, the accepted models, their particularities, features, I defined their advantages and disadvantages, uniformly summarizing and complementing the heterogeneous, usually insufficient and non-consequential lists that can be found in technical literature. I review the definitions given to **governmental clouds** and **I determine** that **there is not a uniformly accepted definition.** As in my opinion **it would have practical benefit, I created my own definition, first on the concept of the governmental cloud, then that of the law enforcement cloud.**

I also clarified the differences among cloud computing and firstly the virtualization of the traditional ICT systems, secondly the outsourced ICT systems and services, and thirdly the services based on Internet technology.

I also determined that currently there is no clear line between the services based on Internet technology and its subset, the Public Cloud / Software as a Service (PC/SaaS) systems, what is more, considering the pace of the appearance of the new services; the new functions they

supply; the possibilities that usually are significantly different from the previous ones that line cannot be drawn for a long time. Regarding the tendencies and the predictions of the industry **I proved that the national security services and law enforcement agencies have to deal with cloud computing because of the possible utilization, the increase of the data security of the protected leaders and the ensuring the lawful monitoring**.

In chapter two **I analyzed and evaluated the public and relevant security recommendations created by the national and international organizations of the developed countries**, such as the CSA's, the FedRAMP's, the BSI's as well as the ENISA's documents, and I revealed the risks required for the assessment of security. **I found that the different organizations examine the given issue in a heterogeneous way**, where three essential differences can be identified at the beginning. The first one is whether they approach the subject **from the service provider's or the user's aspect**, the second whether **the targeted user is civil or governmental organization, or maybe an individual**, and the third is whether the organization who prepared the document originates from **the technical and legal environment of the United States or the European Union. I** also **determined** that even though **none of the organizations examined it in terms of the law enforcement agencies**, the content of these documents with appropriate reconsidering and altering can be used for a security template.

From the recommendations of different organizations on the advantages and disadvantages of the deployment models I concluded that it is the community cloud which is the optimal solution for the law enforcement agencies.

I created a new framework of criteria for the complex security examination of cloud computing systems from the point of view of law enforcement agencies'. This is a four-dimensional space that contains "the role of the law enforcement agency – deployment models - service models – security questions for analysing". I also introduced a new category in the "security questions for analysing", that is "operational reliability, operational safety – data security – other (legal, physical etc.) security – lawful monitoring". In this latter subcategory I defined what issues I regard as operational reliability, operational safety, as data security, as other (legal, physical etc.) security, or as lawful monitoring issues, whether these could be solved in a technical or legal way, and in addition, how the responsibilities and interests are divided between the user and the service provider. With the help of this, any of the mentioned agencies can traverse through a given system's examination concerning any of their tasks.

Using the previously mentioned categories **I created an analysis template** and its manual for t**he law enforcement agencies in order to assess whether the selected cloud computing system can satisfy the minimal required level of security.** I highlighted that thanks to partly the technical development and partly to other needs it can be developed even on its own and using it as a basis, it can be expanded to the unique security subfields according to the examination level with creating newer templates.

I stated that with respect to lawful monitoring it would be practical to introduce and standardize the concept of Lawful Monitoring as a Service (LMaas) (or something like this) in order to provide all the required and claimed information allowed by law to all authorized agencies within unified framework and approach.

In chapter three I analyzed the main issues of the data protection of protected leaders. I highlighted that the TSCM (Technical Surveillance Countermeasures) should be extended to the portable infocommunication devices for personal use and the services based on Internet technology used by the protected leaders. I also determined that **the information security protection cannot or only at an unrealistically expensive way can be evolved, at the same time one of the most sufficient and cheapest ways to protect information is the security-awareness using.** In order to achieve this, a customized training method should be accomplished. By the previous categorization I presented what the relevant risks are, and what effect the users can have on them. **I worked out a personalized basic security-awareness using training method for the protected leaders in order to improve the data protection, with the help of the unfolded risks and the above mentioned framework** in a way that it can be applied to any new services or devices. I stated that this education is necessary but not enough on its own. I find that moving forward is essential in four categories: in case of the tasks that need approach at a higher level, those performed by protected leaders, those performed by operational specialists and those performed by TSCM specialists.

In chapter four I analyzed the possibilities of the lawful monitoring of services based on Internet technology, including PC/SaaS systems. With regard to this, I presented that the technological convergence found in infocommunication devices and services indicates the convergence of lawful monitoring methods, which start fundamental changes in this scope of duties as well.

I proved that the concept of communication in electronic way is more widely interpretable than traditional telecommunication, moreover, the traditional telecommunications forms have been losing their significance to the users and thus to those who perform lawful monitoring. Because **the telecommunication service provider model does not meet the current circumstances, I created a new model, the infrastructure, application and content service provider model, which could replace it.** I also presented that **the services based on Internet technology play a great role in the change of communication in electronic way, but the lawful monitoring of these has legal and technical problems**. I cited international examples from public sources about the currently available means and methods, and then using these sources I classified them, describing their features as well.

I created new, generally applicable criteria for the examination of lawful monitoring methods, then regarding the assessment criteria given here I analysed the currently available methods and summarized their main advantages and disadvantages in a table. By means of this the authorized services can decide on the introduction of a given method as well as they can undertake the analysis of any other, even a completely new monitoring method.

I also made clear that the lawful monitoring of the services based on Internet technology mean a challenge to the concerned body of every country, a reason of which is that none of the methods give a comprehensive solution for obtaining all of the required data, the other reason of which is the insufficiency of the regulation. I proved that the **co-operation with the application service provider is unavoidable, at the same time the most insufficiencies can be found in the regulation of this. It is necessary to define the concerned market participants appropriately, namely the service providers, from the view of lawful monitoring to complement the legal insufficiencies, which definition can be created by means of my infrastructure**, application and content service provider model. After the analysis of the currently available national and foreign definitions **I defined the concept of infrastructure, application and content service providers** in such a way, that they can be integrated in the law and other regulations concerning lawful monitoring. Every service provider and service can be placed in it, but at the same time I emphasize that the concept of traditional telecommunication service provider and service should be kept.

6. NEW SCIENTIFIC RESULTS

1. **I worked out a new complex framework for the examination of** security issues of using **cloud computing systems** in terms of national security services and law enforcement agencies.
2. **I framed a** freely usable **template** and its manual **for assessment of security issues of cloud computing systems for national security services and law enforcement agencies.**
3. **I worked out a possible customized basic awareness training method for protected leaders in order to increase their information security.**
4. **I developed a framework for examination of assessment of lawful monitoring methods of infocommunication systems** establishing the assessment methods for each criteria.
5. Instead of the existing telecommunication service provider model **I worked out a new, infrastructure-, application-, and content service provider model**, which can potentially replace that, and **I defined the infrastructure-, application-, and content service provider**.

7. PRACTICAL USE OF THE RESEARCH RESULTS

- It can be used to increase the safe utilization of infocommunication systems including cloud computing systems by national security services and law enforcement agencies.

- It can help to increase the level of information security awareness of protected leaders.
- It can be used to select an appropriate existing method, as well as to analyse new methods for a particular task of lawful monitoring of an infocommunication system, for empowered bodies for covered information gathering.
- The new model and definitions of service providers can be used to create new legislation of covered information gathering of infocommunication systems.
- It can be used for educational activities in National University of Public Service, as an independent curriculum, as a source of a new research, or as a recommended bibliography.
- It can be used for the awareness programs of GovCERT.

- Particular parts of the dissertation can be adopted for governmental offices, private companies or individuals.
- It can be a base for further scientific researches.

8. RECOMMENDATIONS

I recommend my research results for further utilization:

- for information security specialists of infocommunication systems dealing with cloud computing systems;
- for students and lecturers of the National University of Public Service;
- for legal specialists working on new legislation of infocommunication over the issues of legal monitoring.

9. PUBLICATION LIST OF THE CANDIDATE IN THIS TOPIC

Peer-reviewed journal articles:

1. Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél. Hadmérnök. VI. Évfolyam 4. szám - 2011. december, pp. 176-188. ISSN 1788-1919 Online: http://hadmernok.hu/2011_4_kovacsz.php
2. Kovács Zoltán: Cloud Security in Terms of the Law Enforcement Agencies. Hadmérnök. VII. Évfolyam 1. szám - 2012. március, pp. 144-156. ISSN 1788-1919 Online: http://hadmernok.hu/2012_1_kovacsz.pdf
3. Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. Hadmérnök. VIII. Évfolyam 1. szám - 2013. március, pp. 233-241. ISSN 1788-1919 Online: http://hadmernok.hu/2013_1_kovacsz.pdf
4. Kovács Zoltán: „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" I. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 171-183. ISSN 1788-1919 Online: http://hadmernok.hu/133_17_kovacsz_1.pdf
5. Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 184-197. ISSN 1788-1919 Online: http://hadmernok.hu/133_18_kovacsz_2.pdf
6. Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 198-210. ISSN 1788-1919 Online: http://hadmernok.hu/133_19_kovacsz_3.pdf

7. Kovács Zoltán: „Electronic Written Tasking Order System” Accomplished Within the Project „Secure Electronic Communication” II. Hadmérnök. VIII. Évfolyam 4. szám - 2013. december, pp. 201-209. ISSN 1788-1919 Online: http://hadmernok.hu/134_17_kovacsz.pdf
8. Kovács Zoltán: „Electronic Written Tasking Order System” Accomplished Within the Project „Secure Electronic Communication” III. Hadmérnök. IX. Évfolyam 1. szám - 2014. március, pp. 199-208. ISSN 1788-1919 Online: http://hadmernok.hu/141_19_kovacsz.pdf
9. Gazdag Tibor – Kovács Zoltán: Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei. Nemzetbiztonsági Szemle. II. Évfolyam 2. szám - 2014. június, pp. 36-57. ISSN 2064-3756 Online: http://uni-nke.hu/uploads/media_items/gazdag-tibor-kovacs-zoltan-felho-alapu-uj-penzugyi-tranzakcios-lehetosegek-es-azok-veszelyei.original.pdf
10. Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából I. Hadmérnök. IX. Évfolyam 2. szám - 2014. június, pp. 277-289 ISSN 1788-1919 Online: http://hadmernok.hu/142_26_kovacsz_1.pdf
11. Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából II. Hadmérnök. IX. Évfolyam 2. szám - 2014. június, pp. 290-296 ISSN 1788-1919 Online: http://hadmernok.hu/142_27_kovacsz_2.pdf
12. Kovács Zoltán: Hordozható infokommunikációs eszközök használatához kapcsolódó biztonságtudatossági képzési tematika védett vezetők számára. Hadmérnök. IX. Évfolyam 3. szám - 2014. szeptember, pp. 182-190 ISSN 1788-1919 Online: http://www.hadmernok.hu/143_14_kovacsz.pdf
13. Kovács Zoltán: Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből. Nemzetbiztonsági Szemle. II. Évfolyam 4. szám - 2014. december, pp. 3-28 ISSN 2064-3756 Online: http://uni-nke.hu/uploads/media_items/nemzetbiztonsagi-szemle-2014-4-2.original.pdf (2014.11.27.)
14. Kovács Zoltán: Védett vezetők hordozható infokommunikációs eszközeinek védelme a rádiófrekvenciás tartományban. Bolyai Szemle. XXIII. Évfolyam 2014/4. szám, pp. 58-75 ISSN 1416-1443 Online: http://uni-nke.hu/downloads/kutatas/folyoiratok/bolyai_szemle/Bolyai_Szemle_2014_04_elektron.pdf

Peer-reviewed professional's conference presentation published in conference proceedings

15. Kovács Zoltán: Felhő-alapú informatikai rendszerek, mint nemzetbiztonsági kihívás. Hadtudomány XXIII. Évfolyam 1-2. szám - 2013. március, pp. 5-12 ISSN 1215-4121 Online: http://mhtt.eu/hadtudomany/2013/1_2/HT_2013_1-2_mhtt.pdf

Peer-reviewed professional's conference abstract published in conference proceedings

16. Kovács Zoltán: A Theme of Security Awarness Training for Protected Leaders Concerning the Use of Portable Infocommunication Device / Hordozható infokommunikációs eszközök használatához kapcsolódó biztonságtudatossági képzési tematika védett vezetők számára. In: A haza szolgálatában 2014 konferencia rezümékötet. Szerk.: Kiss Dávid, Orbók Ákos. Nemzeti Közszolgálati Egyetem. Budapest 2014. pp. 160-161. ISBN:978-615-5491--88-7

University textbook chapter

17. Dobák Imre - Kovács Zoltán: Új technológiák hatása a hírszerzésre. In: A nemzetbiztonság általános elmélete. Szerk.: Dobák Imre. Nemzeti közszolgálati Egyetem Nemzetbiztonsági Intézet. Budapest 2014. pp. 206-220. ISBN: 978-615-5305-49-8

10. SCIENTIFIC-PROFESSIONAL BIOGRAPHY OF THE CANDIDATE

Name: Zoltán Kovács
Phone number: + 36 30 520-5993
E-mail: zkovacs@nbsz.gov.hu

Education:

2012 –	National University of Public Service, Military Engineering Doctoral School
2001 – 2004	Budapest University of Economic Sciences and Public Administration, Faulty of Business Administration, area of specialization: Business Economics – Engineer-Economist
1986 – 1991	Technical University of Budapest, Faculty of Electrical Engineering, area of specialization Telecommunication – Electrical engineer
1981 – 1985	Corvin Mátyás Secondary Vocational School on Telecommunication – electronics technician

Language skills:

language	type of exam	Institute
English	intermediate level, type: A + B	State Language Examination Board
English (advanced with military material)	intermediate level, type:B	Zrínyi Miklós National Defense University
French	elementary (B1) combined	Budapest University of Technology and Economics

Main training courses:

2011	Top Senior Police Officer Course TOPSPOC IX – 2011 – European Police College
2011	FBI leadership training course – International Law Enforcement Academy
2005	Senior Executive Seminar – Georg C. Marshall European Center for Security Studies
1994	The GSM an European digital mobile telecommunication system – Technical University of Budapest, Institute for Engineer Further Training
1992	Mobile telecommunication systems – Technical University of Budapest, Institute for Engineer Further Training

Professional experience:

1992 –	Special Service for National Security
1991 – 1992	CANSYS Informatics Ltd.

Budapest, 19 August 2015

Zoltán Kovács