**NATIONAL UNIVERSITY OF PUBLIC SERVICE**

**Doctoral School of Military Sciences**

# THESES

**Dániel Berzsenyi**

**Special Cyber Operations**

**The Analysis of the Cyber Special Operations Capability and its Formation**

**Supervisors:**

General, Prof. Dr. Zoltán Szenes

Brigadier General, Prof. Dr. László Kovács

Budapest, 2022

# Table of Contents

# Introduction

Conflicts are as old as mankind. People have developed a wide range of methods to deal with disagreements stemming from different values and interests, where alongside the peaceful practices, we can also observe different forms of violence. Investigating the history of conflicts, it becomes evident that the impacted parties and their leaders were using a different approach when trying to apply the toolkit at their disposal. Today's toolkit used in international affairs is influenced by the expansion of the security challenges, risks and threats following the collapse of the bipolar world order. The actors pursuing their interests belong to a different cultural background, they have a diverse level of development, resources and perception of security. These influences have led to the rise of asymmetric capabilities, the spread of the hybrid use of traditional and non-traditional warfare and a higher recognition of information- and cyber warfare, and intelligence activities in cyberspace. The later ones also include such sophisticated and complex capabilities and operations that leave us unprotected both on a personal and societal level due to their extensiveness in time and space.

Today's international environment is multipolar while connectedness and mutual dependency are determinative. Because of this, pursuing interests and handling conflicts only with traditional methods is less and less efficient. This is especially true in case of conflicts under the threshold of war and in the "gray zone", covering activities not undertaken publicly in international relationships. The turbulent global political environment of the 21st century poses a significant challenge to the parties of international relationships, blurs the balance of power and the boundaries between the different levels of conflicts, and encourages the creative use of their toolkits to pursue their interests. In the toolkit of pursuing national interests, the perception and strategic embeddedness of the non-traditional method of cyber operational capabilities is diverse. The strategically and technologically more mature actors try to cover the full spectrum of cyber operational capabilities via applying a specialized approach, and operate both defensive and offensive components at the same time. We can draw parallels between the integrated application of these components and the parameters of such well known threats, that the cybersecurity sector associates with the most significant negative impacts and that the scientific research- and professional community have not paid attention to.

When investigating the significance of cyber operational capabilities we need to take into consideration one of its foundational characteristics, its multiplier effect. On the one hand, this can be observed in the physical world during special operational activities, on the other hand, it's especially important for actors with less (cyber) maturity and limited resources. Taking this as a starting point, I am examining the opportunities in cyber operations capabilities from the point of view of small states by creating a unique model combined with the specific parameters of cybersecurity challenges. Within the wide range of cyber operations capabilities, the dissertation is focusing on those special patterns that go beyond regular activities, just like the use of special forces does in physical warfare. From a methodology perspective, the analysis of the process of building up cyber special operations capabilities is made more thorough and informative by the comparison and analysis of three aspects: the strategic documents and embeddedness, the characteristics of special operations activities and the parameters of cyber threats causing the most negative impacts. The research enables us to obtain new scientific findings and valuable information about the international best practices on the field. Therefore my research also aims to identify the requirements and patterns related to the establishment of cyber special operations capabilities.

## Identifying the research problem

While all the metrics related to cybersecurity incidents show a drastic increase, the negative impacts of cybersecurity activities are also becoming more tangible to more and more layers of society. Intermittent services, emptied bank accounts, identity thefts, blackmail with personal data and many other negative effects can already cause serious problems on the individual's level, and it might even trigger a crisis or matter of national security on a societal level. Cybersecurity and cyberdefense professionals have come across an increasing number of events in recent times that were the result of deliberate actions and had serious consequences on a societal level as well. In the background of these events we can often identify interests related to geopolitical tensions and intentions, which not only pose a challenge to the participants of the conflict, but to the international community of the 21st century as well.

The number of international actors recognising the significance and relevance of activities in cyberspace is constantly growing. The effects of activities in- or through cyberspace can be widespread, while due to the characteristics of cyberspace, prevention, defense and accountability is running into limitations. The term "operational capability" has been invoked from the military terminology and its cyber specialized segment is facing such a dynamic growth and technological development, hence it cannot be compared to the application of any conventional capabilities. These call for a specific approach that can place the special cyber operations capabilities in the comprehensive operational spectrum and can apply them efficiently.

On a national level cyber operations capabilities supporting the pursuit- and protection of interests are usually established within the existing armed forces. The official relationship however is rarely straightforward, often hard to detect and almost never can be proven, hence the "state sponsored" terminology has spread. The hybrid character and asymmetric nature of cyberspace enables the multiplication of the applied forces and capabilities, while anonymity is guaranteed to a high level. The incidents and conflicts happening in cyberspace alongside the applied methods and processes can be analyzed from several aspects, similarly to the analysis of the kinetic impacts of incidents and conflicts in the physical space. However, up until now these analyses have not happened, or were carried out in a limited form. A few countries have built up a significant advantage on these fields in the last few years and by now possess such cyber operational capabilities that spans further than their and their allies' defense systems. With their special cyber operations capabilities they can launch precise cyber attacks against any target to achieve social, economic, political, military and national security impact.

In the physical space such impacts are usually generated with operations launched by the specially trained staff of military special forces, law enforcement special units or national security services. Similarly to the physical space, we can identify such operations and capabilities in cyberspace as well that correspond with the special operations capabilities. The special operations forces in cyberspace perform similar activities as their counterparts in the kinetic space, just in a different dimension. Although there is limited information about the cyber operations capabilities of the actors in the international environment, there are several threats to the social system and stability[1],

[1] An example of cyber operations impacting the societal system and stability is the intervention into the 2016 Presidential elections in the US. More information: https://www.cfr.org/cyber-operations/

to economic security[2] or to energy safety[3] that imply the presence of government backed (state sponsored) activities.

Since what appears as a cyber operations capability to one party, is a cyber threat to the other, it is relevant to analyze the question from the perspective of military sciences and to examine the role of cyber operations in international relations, conflicts and during the pursuit of political and national interests. Further analysis is necessary to identify the special types of cyber operations capabilities and to form such units that are able to design and implement these capabilities.

## Research Objectives

In my dissertation I analyze the formation of cyber special operations capabilities on the level of national skill development as part of the national pursuit of interests as one of the possible answers to the emerging threats of cyberspace in the post millennium era. The study focuses on strategic and defense organizational perspectives. I have defined the following research objectives along the foundations of cyber special operations capabilities:

1. Based on the recent strategic documents of cybersecurity and cyberdefense, explore the openly disclosed cyber operational capabilities and level of ambition in Hungary and its neighboring countries where strategic documents are available to the international audience and some selected small states and great powers. Articulate conclusions regarding the limitations of understanding the cyber operational capabilities.
2. Identify those cyber threats that are linked to the most impactful known cybersecurity incidents and use the most sophisticated tools, methods and procedures to achieve their goals. Define the parameters that are equally observable related to the special operations of the defense organizations and the advanced persistent threats as well, with specific attention to those operations that are executed undercover, with outstanding quality, in an organized

[2] An example of cyber operations impacting economic security is the attack on the Society for Worldwide International Financial Telecommunications (SWIFT) system in 2016 through the Bank of Bangladesh. More info: https://www.cfr.org/cyber-operations/

[3] An example of cyber operations impacting energy security is the attack on the Ukrainian energy system in 2016. More information: https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine

and planned manner, aiming to pursue higher - security, military, national security, political - interests.

3. Make a recommendation about the placement of cyber special operations capabilities that include both preventive and counterattack capacity and are essential for detection, prevention and elimination and are proportionate to the threat. The capabilities should be formed within the boundaries of the national capability development as part of the national toolkit to pursue interests to guarantee more efficient pursuit of interests.
4. Based on the similar patterns and rulesets of cyber operations- and special operations capabilities, elaborate on the opportunities and requirements of the establishment of cyber special operations capabilities on the full spectrum of cyber capabilities, with special focus on the application of resources.

## Hypothesis

In accordance with the research objectives I examined three hypothesis and their components:

> H1: In the current strategic environment, states do not, or only partially disclose openly their cyber operational capabilities and the full spectrum of these capabilities entail the necessary preventive and counterattack capacity needed for a proportionate response.
>
> H2: Several traits of known Advanced Persistent Threats (APT) show similarities and can be set parallel to the capabilities of special operations forces applied in the kinetic domain.
>
> H3: It is possible to create a framework that covers the full spectrum of cyber capabilities including the elements that enable preventive and counterattack operations, which can be achieved by applying a specific approach similar to the one used for kinetic special operations capabilities.

The examination of the first hypothesis (H1) was carried out with a security and defense policy approach, based on an analytical-evaluating review of strategic documents that are in force at the time of the writing of this dissertation in Hungary and in the neighboring states with internationally available strategic documentation (Austria, Croatia, Slovakia, Slovenia, Ukraine), in four smaller

states chosen based on their high maturity in cybersecurity and the existence of advanced cyber security capabilities (Israel, Estonia, Switzerland and The Netherlands) and in three major powers (China, United States and Russia). The part of the dissertation focusing on the first hypothesis also answers the question on a strategic level "What level of ambition do the examined states and organizations disclose in terms of openly developing cyber defense capabilities?".

The investigation of the second hypothesis (H2) is executed based on professional interviews and the comparison between the defense organizations' special operations capabilities and activities, and the patterns and regularities of advanced persistent threats. The analysis reveals several similarities triggered by the undercovered execution, with outstanding quality, in an organized and planned manner, aiming to pursue higher - security, military, national security, political - interests. The part of the dissertation focusing on the second hypothesis also answers the question "Could APTs acting with the necessary political authorization in order to protect national interests be considered cyber special operations forces?"

The examination of the third hypothesis (H3) is based on the processed primer and secunder expert resources and the system of conditions evolving after the expert interviews. The system of conditions - focusing on the level of national capability development - enables identifying the resources needed for establishing the cyber special operations capabilities and describing their application methods. The part of the dissertation focusing on the third hypothesis also answers the question "What elements does a framework need to have to guarantee the formation and development of cyber special operations capabilities?"

## Methodology

The dissertation mostly relied on deductive methodology, which enables a comprehensive approach and processing of the publicly known cybersecurity events and trends in the post millennium era. In order to reach the research goals, there were several methods applied from the general research methods, such as analysis, synthesis, critical adaptation, some quantitative, but mostly qualitative research, and comparative methods. In terms of the specific methodologies of military science research, I have applied my own cyber threat intelligence and cyber security

incident indicators (Indicators of Comromise - IOC) related experience utilization and categorisation.

As the first step, I aimed to evaluate the strategic perspectives and goals related to cybersecurity and cyberdefense. I have gone through an extensive literature review and analyzed and compared the level of ambition of the respective states in terms of the cyber capabilities discussed in the strategic documents. The primer resources have only provided a limited opportunity to synthesize the perception of the level of exposure to the threats and the level of security. Therefore, I have used several secondary sources to analyze publicly available information about APTs while I was looking for connections with more mature national cyber capabilities. Based on the analysis, including a process analysis method, I have prepared three case studies to demonstrate the analogies between the cyber operational capabilities of major powers and advanced persistent threats. By analyzing documents further and applying a comprehensive approach, I examined, interpreted and arranged the full spectrum of cyber operations from defensive to offensive components, including the openly undisclosed "gray zone" operations. After defining the cyber operations capabilities and preparing the case studies, I incorporated the special operations forces and capabilities used in the kinetic domain, then compared their operational parameters with the attributes of APTs using a dominance based analysis. Furthermore, through processing the strategic and operational perspectives in a unified framework and taking into consideration the regulatory background, the democratic control and the efficiency criteria, I have analyzed the options for the formation and placement of cyber special operations capabilities and introduced potential organizational integration alternatives. To create a framework for describing the elements of the cyber operations capabilities that are able to fulfill preventive and counterattack tasks, I mostly relied on literature analysis and guided expert interviews.

All materials used in the dissertation have been listed in the *Literature* section. To clarify the basic terminology and definitions, such primarily primer sources were used (rules of law, strategic documents, codes and manuals of international organizations, military doctrines etc. ) that are widely accepted due to their maturity, international recognition or other characteristics. Discussing terminological disputes was intentionally avoided, hence I directly quoted and applied the definitions from the above mentioned sources or created working definitions of my own in case it

was necessary. Hungarian an foreign (mostly English) abbreviations are often used, but all of these are listed in the *Abbreviations* section in both Hungarian and English.

## Summary of the analysis

The dissertation consists of ten chapters. The first chapter introduces the research, reviews the research problem, the objectives, the hypothesis, the research methodology and the literature review.

The second chapter defines the theoretical framework in seven subchapters. First the global commons and the timeframe are introduced, followed by describing the challenges of cybersecurity and defense organizations in the 21st century. This is accompanied by the review of the relationship between contemporary armed conflicts and cyber warfare. The last two subchapters explore the connections among national capability development, national interests, the pursuit of national interests and cyber operations.

As the first step of the analysis of the cyber operations capabilities, the third chapter contains the inspection of the strategic cybersecurity documents, focusing on the cyber capabilities of the neighboring countries and the selection of a few small states and three great powers. Afterwards, the chapter discusses the exploration and arrangement of all capabilities within the full spectrum of cyber operations. The third element of the chapter is the case studies describing the development of cyber operations capabilities.

The fourth chapter focuses on advanced persistent threats (APTs). The first part of the chapter concentrates on the interpretational framework and basic knowledge about APTs. It examines in detail the parameters and characteristics of APTs, introduces the options for categorisation, discusses the details of the state sponsoration and circumstances and requirements of efficiency, and finally describes the difficulties in terms of identifying APTs and their members. The second half of the chapter provides a detailed analysis and evaluation of APTs based on the level of development, persistence and threat. Using these learnings it defines those parameters that can be used to draw parallels and find differences with the kinetic special operations forces and capabilities.

The fifth chapter focuses on analyzing the special operations capabilities of defense organizations. Via creating and applying a unified framework, it examines the tasks of the military special operations forces, law enforcement special units and national security services special capabilities, the operational circumstances and characteristics, and the connection between training, arms drill and the requirements. The connections and parallels among the most common parameters of the tasks related to the special capabilities are summarized in a table that also contains the identical parameters of APTs to enable the dominance based comparison.

| SPECIAL OPERATIONS CAPABILITIES | COVERED NATURE | | SIGNIFICANCE | | | OPERATIONAL FIELD | | OPERATIONAL CYCLE | | TARGETED | ADAPTIVE | SPECIAL RESOURCES | SPECIAL REQUIREMENTS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | DISCLOSED | DENIABLE | HIGH PROFILE | STRATEGIC | POLITICAL | HOMELAND | FOREIGN LAND | SHORT | CONTINUOUS | | | | |
| MILITARY | ● | ● | ◑ | ● | ● | ○ | ● | ● | ◑ | ● | ● | ● | ● |
| LAW ENFORCEMENT | ● | ○ | ● | ○ | ◑ | ● | ○ | ● | ◑ | ● | ● | ● | ● |
| NATIONAL SECURITY | ◑ | ● | ● | ● | ● | ● | ● | ◑ | ● | ● | ● | ● | ● |
| ADVANCED PERSISTENT THREATS | COVERED NATURE | | SIGNIFICANCE | | | OPERATIONAL FIELD | | OPERATIONAL CYCLE | | TARGETED | ADAPTIVE | SPECIAL RESOURCES | SPECIAL REQUIREMENTS |
| | DISCLOSED | DENIABLE | HIGH PROFILE | STRATEGIC | POLITICAL | HOMELAND | FOREIGN LAND | SHORT | CONTINUOUS | | | | |
| STATE SPONSORED APT-S | ○ | ● | ● | ● | ● | ○ | ● | ◑ | ● | ● | ● | ● | ● |

Figure 5: The dominance based analysis of the characteristics of military, law enforcement and national security special operations capabilities and advanced persistent threats[4]

The sixth chapter contains an extensive review of the cyber special operations forces in seven subchapters. The first subchapter discusses the raison d'etre of the cyber special operations forces based on operational and strategic perspectives, and the mid-term challenges of cyber operations. Then the second chapter continues with introducing the formation and operational background. Therefore it specifically mentions the dilemmas related to the operational boundaries, the role and significance of the democratic control and the need for immediate action. The third chapter evaluates the options for the organizational integration of cyber special operations forces using four different models. The fourth subchapter deals with the recruitment and selection of the executional staff, including the process of defining the necessary knowledge, skills and capabilities. The fifth

[4] The figure is the work of the author.

subchapter introduces a new model relying on specific elements of the preparation and training, the necessary infrastructure and the expectations towards the preparation. The model enables the indicator based representation of the full spectrum of the cyber operational capabilities.

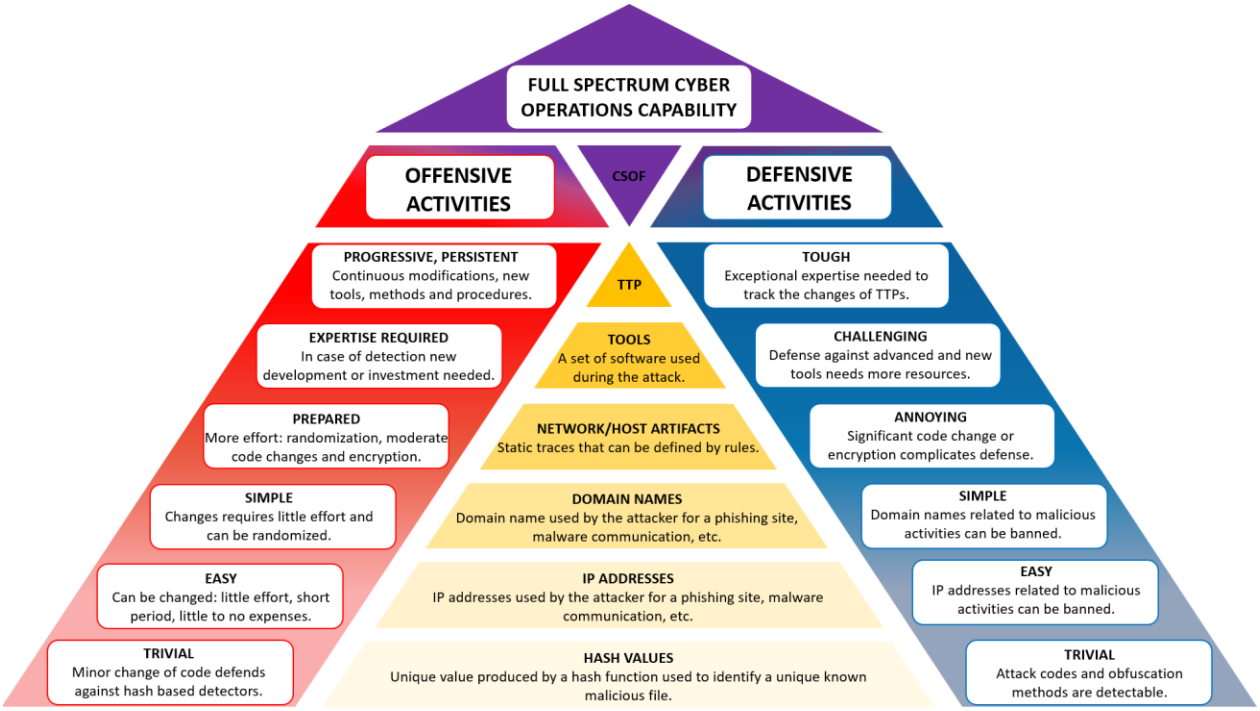


Figure 8: The schematic representation of the model of full spectrum cyber operational capabilities and cyber special operations forces based on the indicator focused scaling of offensive and defensive activities

The last two subchapters deal with the three most important components of cyber special operations, the necessary resources and the emerging risks and challenges.

The seventh chapter contains the summarized conclusions, while the ninth presents the usability of the scientific results of the dissertation. The tenth chapter is divided into two parts, and covers the recommendation for scientific research and political follow-ups.

## Summarized Conclusions

As the result of the review of cyber security strategies I concluded that states usually do not provide precise information about their cyber operational capabilities and the documents often do not contain straightforward definitions for the applied terminology. Therefore on the level of strategic

documents the boundaries between the different segments of cyberdefense and cyber operations, and the circumstances of their application are blurred. I came to the conclusion that in most of the countries, it is hard to define solely based on the cyber strategies, what activities were meant exactly, and whether and if yes, how, the military, law enforcement and national security sectors are impacted when cyber operational capabilities are being mentioned. While for international organizations, the defensive nature is clearly dominant on a strategic level, in case of great powers and smaller states that are more developed from a cyber perspective, offensive capabilities are often named or directly referred to. The majority of the examined strategies though take a precautionary approach and emphasize the defensive aspect of the cyber operational capabilities.

The examination of cyber operational activities highlighted the existence of such frameworks that can describe the components of the cyber operational capabilities and define those technical and ethical aspects that can be used to separate the defensive and offensive capabilities. Analyzing various aspects of cyber operations, I have come to the conclusion that passive and active defense and offensive activities most of the time can be separated based on a few parameters, however the boundaries are often blurred. This is especially true for activities and operations that consist of more elements. In these occasions, the result is a hybrid operation with both defensive and offensive elements, that entail special capabilities as well alongside the traditional ones. I determined that cyber operations containing a limited number of special or offensive elements can be deemed defensive from the aspect of their final goal. There is no internationally accepted practice, standard or regulation. Actually, this is the so-called “gray zone” that certain strategies refer to and where more and more states try to perform efficiently. It is visible from the case studies that the three decisive geopolitical actors of the multipolar world have recognized the significance of cyberspace and are carrying out decades-long projects related to the formation of cyber operational capabilities. Even though they openly support the expansion and development of the international regulations, in reality they try to exploit the nature of cyberspace to achieve their power ambitions and pursue the national interests.

As the result of analyzing APTs I have determined that they have precise and clear goals, they demonstrate a high level of organization and have access to significant resources, while their activities are spread over a longer time period and are often repetitive. Activities that can be linked to APTs usually become public related to a high impact incident executed to pursue strategic and/or

political interests. Furthermore, the activities are sophisticated, hard to detect and use adaptive technical solutions. As a result they are able to stay anonymous for an extended amount of time. During the analysis of APTs I have separately examined the most important characteristics as well. From examining the level of advancement I could point out that APTs are capable of using and exploiting such technologies during their activities that require special knowledge and on occasions extreme levels of creativity. Examining persistence revealed that APT activities are able to remain undetected on the victim's computer system and networks for hundreds of days. APT activities usually entail recurring surveillance and data theft combined with a high level of reactive capabilities. During the analysis of APTs I have determined that their activities have proven several times that they can generate impact crossing the boundaries between the virtual and physical world, hence they pose a significant threat to the political-social order of the states. They are capable of obtaining and manipulating sensitive information, or causing disruption along geopolitical, economic, security and other goals, while deniability is present to such a high level, that no physical operation can compete with.

After defining several parameters related to the activities of APTs that even respectively can significantly increase efficiency, I compared these to the parameters of the special operations capabilities of the defense sector. Following the analysis I determined that the special capabilities of the specific areas can be clearly distinguished based on the sectors and activities, however there are overlaps that indicate a tight relationship and knowledge transfer on occasions. I started the examination of the raison d'etre of cyber special operations forces with the challenges of the kinetic special operations forces, which shows a dual picture in the sense that while in Hungary it's not imaginable to form a robust cyber operations capability within the special forces, in the United States there is already active debate about forming the units participating in cyber missions under USCYBERCOM or USSOCOM. Via reviewing the strategic and operational levels, I have pointed out that the state of the international system and the opportunities provided by cyber space generated such behavioral patterns in some states, that cannot be tracked and controlled by the international law frameworks, hence in case interests are harmed, the traditional response toolkits are significantly limited.

I have determined that the formation of capabilities that can be applied on the full spectrum of cyber operations can be interpreted as a response to the anarchic state that evolved in the cyber

dimensions of international relations, which is most often referred to nowadays as the “cyberwar” of the great powers. Even though from the point of view of military science using the war narrative is incorrect, the cyber operational capabilities of governmental and state sponsored organizations explored in the research clearly reach a level, where they can generate impact comparable to kinetic attacks, only faster and in a more cost efficient way by maximizing the utilization of the asymmetries of cyber space.

I have examined several alternatives to understand which integration schemes offer a high level of efficiency, simple embeddability or deniability during the formation of cyber operations capabilities. I have determined that the military, the national security, the paramilitary and the contractor models all have several advantages and disadvantages as well, which need to be taken into consideration by all parties before forming the capabilities to be able to choose the most suitable solution. Based on the interviews and the literature review, the robust organizational background and hence the complicated hierarchy and slowness make military and national security integrations less preferable than the self-reliant paramilitary or contractor model. However, further research and evaluation is needed in all scenarios to create a more accurate picture of the advantages and disadvantages in the specific environment where the capability is being formed.

## New scientific results

My dissertation examining the cyber special operations capabilities comprise the following new scientific results:

**1.** Using a targeted, qualitative analysis of cyber security strategies I explored the parts of the documents that are relevant to cyber operations capabilities, summarized the information indicating the offensive or defensive nature of cyber operations capabilities and based on the experiences drew conclusions about understanding the limits of the real cyber operations capabilities and the level of ambition.

**2.** I have identified the advanced persistent threats among the cybersecurity challenges and have confirmed that the worst known cybersecurity incidents can be linked to them, and that they use the most sophisticated tools, methods and procedures to achieve their goals. Using these learnings,

I have defined the analogies between the defense, law enforcement and national security sectors' special operational circumstances and the operational parameters of advanced persistent threats. Then I used these analogies to create a system of conditions for the cyber special operational activities.

**3.** I verified the raison d'etre of cyber special operations capabilities and in order to improve the efficiency of the pursuit of interests, I have made a recommendation for the placement of cyber special operations capabilities on the level of national capability development as an element of the toolkit of national pursuit of interest.

**4.** I have conducted a comparative evaluation of the specifications of the cyber special operational capabilities and the special capabilities of the defense, law enforcement and national security sectors. I have highlighted those parameters that could provide a basis for the formation of the organizational integration, structure and set of conditions and I have created the indicator based model of full spectrum cyber operations.

## The usability of the research- and scientific results of the dissertation

The results of the dissertation can be used in the following areas:

- Policy: The dissertation forms a strategic level picture of the approach towards cyber operational capability development and the types of cooperation opportunities. It explores the embeddedness of the cyber operational capabilities in the security and defense sector of the observed countries on a strategic level, and the national perception related to cyber threats. In relation to this, cyber operational capabilities are not documented in open and accessible sources, hence conclusions can only be made in an indirect manner. These don't apply to specific capabilities, but rather refer to the nature of application. This nature is determinative when evaluating cyber operations as threats or capabilities as well. Based on this, advanced persistent threats can be interpreted as a special element of cyber operations capabilities and can be set parallel to the kinetic special operations capabilities. This knowledge helps the formation of the cyber special

operations capabilities, the establishment of the necessary set of conditions and the acceleration of the related planning processes. Awareness related to the processes and methods of countries who have already successfully formed and applied cyber special operations capabilities increases the efficiency of political planning and decision making and supports the necessary coordination activity, while identifying their disadvantages contributes to avoiding negative factors.

- In applied research: The dissertation deals with the cyber special operations capabilities, which in Hungary has barely been researched before, hence it is primarily exploratory, and secondarily synthesizing, analytical and evaluative building on international literature. Its qualitative and comparative research methodology - primarily in terms of the strategic analysis, the advanced persistent threats and special operations capabilities - is novel in military science, and it summarizes the synthesis of the research findings and practical experience of the author and the interviewed experts. It can provide a sample and methodology basis for research with similar focus and thematics.
- In education and training: Bringing the international literature explored during the research into the field of military sciences, security and defense policy and cybersecurity and special operations education provide such new learnings to the experts of the future in the defense sector and beyond, that are already in great demand on the short term due to the lack of cyber professionals. The majority of knowledge and sources used in the dissertation can only be found in a foreign language, hence were not present in the Hungarian literature and can be used to refresh related training thematics.

# List of the Author's Related Publications

BERZSENYI Dániel: Kiberbiztonság. In: TÁLAS Péter Henrik – CSIKI Tamás – ETL Alex – BERZSENYI Dániel (ed.): *A globalizált világ kihívásai*. Nemzeti Közszolgálati Egyetem, Ludovika Egyetemi Kiadó, Budapest, 2021, p. 341-358.

BERZSENYI Dániel – EDEGBEME-BELÁZ Annamária: Hungary's evolving cyber security strategy. In: MANJIKIAN Mary – ROMANIUK Scott N. (ed.): *Routledge Companion to Global Cyber-Security Strategy*. Routledge, London, 2021, p. 99-110.

BERZSENYI Dániel: A kibertér aktuális nemzetközi biztonságpolitikai kihívásai. In: BERZSENYI Dániel – BODÓ Attila Pál – KAPITÁNY Sándor – SÁGI Gábor János – SEBŐK Viktória (ed.): *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2017*. Dialóg Campus Kiadó, Budapest, 2017, p. 6-22.

BERZSENYI Dániel – EDEGBEME-BELÁZ Annamária: Kiberbiztonsági Stratégia 2.0: A kiberbiztonság stratégiai irányításának kérdései. *SVKK Elemzések, 2017/3*. [online], Access: https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/svkk-elemzesek-2017-4-harom-evvel-az-ukrajnai-hatalomatvetel-utan-talas-p.original.pdf [2022. 07. 16.]

BERZSENYI Dániel: Globális kihívás, regionális válaszok: kiberbiztonság Kelet-Közép-Európában. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 10. évf., 2017/3. szám, p. 69-79.

BERZSENYI Dániel: A kiberbiztonság humán oldala. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 10. évf., 2017/2. szám, p. 54-67.

BERZSENYI Dániel – VÁNYI Rajmond: Egy katonapolitikai döntés lehetséges kiberbiztonsági következményei: az Iszlám Állam elleni magyar katonai szerepvállalás margójára. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 8. évf., 2015/3. szám, p. 134-143.

BERZSENYI Dániel: New dimension in V4 defense cooperation. A comparative analysis of the cybersecurity strategies of CECSP countries. Visegrad Plus – Forum for Visegrad+ Studies. 2015. 01. 18. [online] Access: https://web.archive.org/web/20160611071807/http://visegradplus.org/analyse/new-dimension-v4-defense-cooperation-comparative-analysis-cybersecurity-strategies-cecsp-countries/ [2022. 07. 22.]

BERZSENYI Dániel: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 7. évf., 2014/6. szám, p. 110-136.

BERZSENYI Dániel – SZABÓ I. László: A védelmi szektor néhány elemének transzformációja. In: TÁLAS Péter Henrik – CSIKI Tamás (ed.): *Magyar biztonságpolitika 1989-2014 - Tanulmányok*. Nemzeti Közszolgálati Egyetem, Nemzetközi Intézet, Budapest, 2014, p. 37-58.

BERZSENYI Dániel – SZENTGÁLI Gergely: STUXNET: a virtuális háború hajnala. *Biztonságpolitika: Biztonságpolitikai Szakportál*, Budapest, 2010. [online] Access: http://www.biztonsagpolitika.hu/?id=16&aid=932&title=STUXNET:_a_virtu%C3%A1lis_h%C3%A1bor%C3%BA_hajnala [2022. 07. 16.]

# Short Academic Biography of the Author

Daniel Berzsenyi has conducted his studies at the Miklós Zrínyi National Defense University between 2005 and 2010, majoring in security and defense policy. He took 1st place at the National Scientific Student Conference in 2008. He commenced his PhD studies in 2014 at the Doctoral School of Military Sciences at the National University of Public Service. In 2016 he won a scholarship to do research at the Technical University of Tallinn, where he was investigating the level of digital development and cybersecurity orientation in the Baltic states. Cyber operations capabilities became the focus of his research, hence he chose to write his PhD dissertation on this topic as well.

Related to his research profile, he obtained the *Digital Forensics Technology and Law* certificate in Tallinn, passed the *Certified Information Security Manager* (CISM) examination in 2018 and gained the *ISO 27001 Lead Auditor* qualification. He graduated from the cybersecurity department of the János Neumann Faculty of Information Technology of the Óbuda University in 2020, where he also attended the *White Hat Certified Defender* (WHCD) training.

Alongside his PhD research, he was active in the field of security policy and cybersecurity. During 2015-2016 he was an external contractor at the Institute for Strategic and Defense Studies and the IT security consultant of a startup focusing on identity and access management. Between 2016 and 2019 he worked as a senior cyber threat intelligence analyst in an international cybersecurity team at a multinational financial institution. In 2019 he became a co-founder of a startup dealing with cybersecurity awareness raising, while he keeps working as an independent cybersecurity consultant and advisor. His scientific work was both published in Hungarian and English, and primarily focused on the strategic and operational questions of cyberspace. He is the co-author of a cybersecurity essay book published in English and the co-editor of a security policy essay book in Hungarian. He has an advanced level language certificate in German, and a mid-level one in English. He uses English daily during his work and research activities.