RESEARCH
www.commprac.com
ISSN 1462 2815

# THREATS TO NATIONAL SECURITY AND CYBERCRIME IN COUNTRIES IN TRANSITION - THE CASE OF NORTH MACEDONIA

**Besim Mulaj [1] and Naser Rugova [2]**

[1] PhD, Agency for the Management of Monuments and Memorial Complexes, Prishtina, Kosovo. Email: besim.mulaj@rks-gov.net
[2] MD, PhD, Department of Medical Sciences, University for Business and Technology, Kalabria, 10000, Pristina, Kosovo. Email: naser.rugova@ubt-uni.net

**DOI: 10.5281/zenodo.13347825**

**Abstract**

**Introduction -** In the context of globalization and technological advancement, national security has become increasingly intertwined with cybersecurity. For countries in transition, such as North Macedonia, the challenges are multifaceted. This abstract delves into the threats to national security posed by cybercrime in North Macedonia, highlighting the complexities faced by transitional nations. **Aim -** The primary aim of this study is to explore and analyze the specific threats to national security arising from cybercrime in North Macedonia. Additionally, it seeks to understand the broader implications for other countries in transition. **Methodology** - We have applied a multidimensional approach with a mixed research methodology, using the literature review of the relevant field, qualitative, analytical and comparative methods applied in security science research. 200 respondents were interviewed using the questionnaire as an instrument for conducting the research. **Results** - Cyberspace today is one of the major legal challenges that has sparked another form of crime by creating an environment for new crime methods. Cyberspace today is one of the major legal challenges that has sparked another form of crime by creating an environment for new crime methods. Results of this paper consist on identification of key threats: The study identified several key cyber threats to national security in North Macedonia, including: Cyber espionage targeting government and private sector entities. **Conclusions** - Looking at this prism we can conclude that all state institutions should increase interstate cooperation where they are carriers of the activities that is defined by the strategy therefore, all institutions should reflect an interstate and inter-institutional readiness to have a coordination between those security institutions because it is finally understood by cooperating and coordinating all the institutions can succeed successfully of cyber-attacks that can happen at any moment and attack different institutions or different states.

**Keywords:** Cybercrime, Cyber Strategy, National Security, Cyber Space, Legislation, Cyber War.

## 1. INTRODUCTION

In the modern digital age, national security is intricately tied to the realm of cyberspace. Cybernetic crime, often referred to as cybercrime, encompasses a wide range of illegal activities that are conducted through digital means. These crimes can pose significant threats to national security, affecting critical infrastructure, government operations, economic stability, and societal well-being.

The proposed definition of cybercrime is: “The use of cyberspace for illegal ends, while exploiting unique cyberspace features, such as speed and immediacy; remote operation; encryption and obfuscation, making it difficult to identify the operation and the operator”, (Tabansky, 2012).

Cybercrime, as a relatively new phenomenon, is defined in criminal legal doctrine as a crime where computers are used as tools to commit an offense, and the primary targets are computers and computer systems (Kroci, 2023).

The cybercrime threat is considered as one of the main threats for national security in XXI century. Precisely, the actual core importance in this aspect, assaults against

informative systems of private, state and international organizations, organized in most of the cases by organized transnational criminal organizations, during the periods of armed conflicts or tense situations by state authorities, raised a specific importance to the cyber threats in these current historic moments, because of the increased probability of terrorist attacks and assaults during armed conflicts, to be focused towards information systems and structural information strategically vital for the defense of NATO and EU member states (Nuredini, 2014).

Cyber-attacks can take various forms and cybercriminals have become increasingly sophisticated in the way they launch these attacks. As such, it's vital for business and government institutions to ensure they're familiar with the latest cyber threats and how best to respond to them (The University of Tulsa, 2024).

Cybercriminals are often motivated by financial gain, but there are also instances of politically motivated cyber-attacks, particularly around election times or during periods of political unrest.

Common cybercrimes in North Macedonia include phishing, hacking, online fraud, identity theft, and the spread of malware. These crimes target both individuals and institutions.

Information and communication technologies in Macedonia have experienced a phenomenal growth throughout the last decades, which has had a tremendous impact on governmental services' presence in the Internet, as well as on everyday life. Against this background, technologies-based growth introduces new risks and threats to the cyber domain in the country (Tasevski, 2015).

Common cybercrimes in North Macedonia include phishing, hacking, online fraud, identity theft, and spreading malware. These crimes target both individuals and institutions, which is also the core issue of this research with different focus groups of respondents.

## 2. LITERATURE REVIEW

Strengthening the national capacities for cyber threat management and improving the cyber security have become a priority for the Republic of Macedonia.

The National Cyber Security Strategy of the Republic of Macedonia is a strategic document that fosters the development of safe, secure, reliable and resilient digital environment, supported by high-quality capacities, based on cooperation and trust in the field of cyber security (CCDCOE, 2018).

Although the geography of cybercrime attacks has been documented, the geography of cybercrime offenders–and the corresponding level of "cyber criminality" present within each country–is largely unknown. A number of scholars have noted that valid and reliable data on offender geography are sparse (Kigerl, 2011). Despite the threat it poses, cybercrime is somewhat an invisible phenomenon. In carrying out their virtual attacks, offenders often mask their physical locations by hiding behind online nicknames and technical protections. This means technical data are not well suited to establishing the true location of offenders and scholarly knowledge of cybercrime geography is limited (Bruce at al, 2024). The Index, published in the journal PLOS ONE, shows that a relatively small number of countries house the greatest cybercriminal threat. Russia tops the list, followed by Ukraine, China, the USA, Nigeria, and Romania. The UK comes in at number eight (University of Oxford, 2024). In

Mapping the global geography of cybercrime with the World Cybercrime Index, Macedonia does not appear at all as a country with the most danger from cybercrime.

North Macedonia has a solid legal infrastructure in terms of protection from cybercrime threats. In addition to the national strategy against the threats of cybercrime, there are also some basic laws in force that regulate this field, such as:

Criminal Code, (The Official Gazette of R.M, 2012).

Law on Criminal Procedure, (The Official Gazette of R.M, 2012).

Law on Electronic Communications (The Official Gazette of R.M, 2013).

Law on Communications Monitoring (The Official Gazette of R.M, 2012).

Law on e-Commerce, (The Official Gazette of R.M, 2014).

Law on Electronic Management (The Official Gazette of R.M, 2011).

Code of Civil Procedure (The Official Gazette of R.M, 2010).

Law on Electronic Data Form and Electronic Signature, (The Official Gazette of R.M, 2008) and

Declaration on Safer Internet.

The Republic of North Macedonia has an institutional structure organized as responsible authorities for preventing and fighting cybercrime. the responsible actors, linked in a crisis management system (CMS), include: The Ministry of Interior, the Ministry of Defense, the Protection and Rescue Directorate, the Crisis Management Centre, the Ministry of Transport and Communication, the Directorate for Protection of Classified Information and the Ministry of Environment and Spatial Planning. Other relevant legislation concerns the Ministry of Information Society (Hadji-Janev, 2014).

North Macedonia has harmonized part of the legislation with EU laws and directives. EU law on cybercrime, the main ones are: Council of Europe Convention on Cybercrime (Council of Europe, 2004), Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse (European Commission, 2020), Directive on non-cash payment (European Commission, 2019), Regulation and Directive facilitating cross-border access to electronic evidence for criminal investigations (European Commission, 2018), Directive on attacks against information systems (European Commission, 2013), Directive on combating the sexual exploitation of children online and child pornography (European Commission, 2011). North Macedonia is a signatory party to the states invited to join the Budapest Convention on Cybercrime (Council of Europe, 2023).

## 3. METHODOLOGY

This study employs a mixed-methods approach, combining qualitative and quantitative research methods. Data were collected through: Literature Review: An extensive review of existing literature on cybercrime and national security in transitional countries.

Surveys: Questionnaires distributed to a broader audience to gather quantitative data on perceptions and experiences related to cyber threats. 200 respondents were interviewed using the questionnaire as an instrument for conducting the research.

Case Studies: Analysis of specific instances of cybercrime in North Macedonia to provide detailed insights.

## 4. RESULTS

The survey questionnaire was adapted for a group of 200 citizens, of whom 200 are citizens of the Republic of Macedonia are asked to be persons who are well acquainted with the position and the security background and that of Human rights and threats from cyber chemistry, such as the right to human security. Also featured by experts dealing with the study of international terrorism and security in the protection of human rights, along with the rights of citizens and the threats or threats to cybercrime that has disturbed contemporary society.

**Table 1: Forms and Means of Cyber crime**

| Forms and Means of Cyber crime | Rarely or often | It did not happened | Total |
|---|---|---|---|
| Identity theft online | Yes-no | 4 | 5 % |
| Hacking (illegal access to systems Computer, etc.) | No-yes | 9 | 10 % |
| Throwing of viruses | No-yes | 14 | 15 % |
| Illegal computer data interception | Yes-no | 19 | 20 % |
| Theft of intellectual property online | Yes-no | 10 | 11 % |
| Trafficking of online pornography | | 6 | 6 % |
| Intentional system failure or Computer data | Yes-no | 9 | 9 % |
| (Cyber-Espionage) | No-yes | 6 | 6 % |
| Abuse of children through the internet that has resulted in abuse of real life | No-yes | 11 | 11 % |
| Other crimes | Yes-No | 7 | 7 % |

**Table 2: Defense barriers and infrastructure against cybercrime**

| Questions | Nu. of responds | Number of responses adjusted to (%) percentages |
|---|---|---|
| a).Yes there are many barriers Po, | 55 | 33 % |
| b).There are no barriers | 23 | 11 % |
| **c).** We are not informed | 122 | 56 % |

**Table 3: How much does the state carry out cybercrime training for specialists in this field?**

| Questions | Number of Answers | Number of responses adjusted to (%) percentages |
|---|---|---|
| a). I have no idea | 21 | 10 % |
| b). Yes, | 120 | 55 % |
| c). Should continue | 59 | 35 % |

**Table 4: Assessments related to national strategies for the protection and prevention of cybercrime**

| Questions | Number of responds | Number of responses adjusted to (%) percentages |
|---|---|---|
| a). Yes, it exists | 69 | 36 % |
| b). Exists but results are seen | 109 | 54 % |
| c).I have no idea | 22 | 10 % |

**Table 5: The frequency of cyber-attacks against the state of the Republic of Macedonia or other institutions according to the respondents**

| Questions | Number of responds | Number of responses adjusted to (%) percentages |
|---|---|---|
| a). Yes there have.. | 20 | 10 % |
| b).No there haven't | 110 | 55 % |
| **c**). I have no idea | 70 | 35 % |

### 4.1. Analysis of the results obtained from the survey questionnaire

Based on the study conducted in the framework of this paper, after identifying the main challenges and issues of the state in the fight against cybercrime, based on the analysis of the legal framework, the achievements so far, the statistics and the results obtained from the interviews conducted with specialists responsible for investigating, prosecuting and combating cybercrime were able to come up with some recommendations to be followed by the state to improve the current situation regarding cybercrime in Macedonia.

The respondent had different opinions and that their share of the experiences or obstacles they faced had a bitter experience and that any future action could be even the risk of cyber criminals, we have consistently defined some of the criminal offenses that citizens have suffered in general and from which acts may be victimized and threatened and endangered by cybercrime; Online identity theft 5%, Hacking illegal access to computer systems 10%, Virus Throws 15%, Illicit Computer Surveillance 20%, Intellectual Property Laundering 11%, Trafficking in Online Pornography 6% Cyber-Espionage Data Spam 11% Child Abduction via the Internet that has resulted in 11% of real-life abuse, as well as a number of child pornography online 9%, Intentional Computer Systems or Data Damage 6% Other crimes of 7%, which are of internal character and do not show them for security issues or individual discretion.

## 5. CONCLUSIONS

The findings underscore the urgent need for North Macedonia to enhance its cybersecurity measures. Recommendations include:

Investing in modern cybersecurity technologies and infrastructure. Enhancing the skills and capabilities of cybersecurity professionals through training and education. Strengthening legal and regulatory frameworks to effectively combat cybercrime. Fostering international cooperation to tackle transnational cyber threats. For countries in transition, the study emphasizes the importance of a comprehensive and adaptive approach to cybersecurity to safeguard national security in the digital age.

**References**

1) Tabansky. L, (2012). "Cybercrime: A National Security Issue?", Military and Strategic Affairs | Volume 4 | No. 3, available at: https://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/SystemFiles/MASA4-3Engd_Tabansky.pdf .

2) Kroçi V. (2023), "Kosovo's Take on Cybersecurity", Prishtina, Kosovo: Securitybrief, Available from: https://qkss.org/images/uploads/files/Security_Brief_-Vesa_Kroci.pdf/ .

3) Nuredini. A, (2014), "Challenges in combating the cyber crime", Mediterranean Journal of Social Sciences, available at: https://www.richtmann.org/journal/index.php/mjss/article/view/4294/4200 .

4) The University of Tulsa, (2024), “Cybersecurity Defense Strategies: The Role of Cybersecurity in National Security”, available at: https://online.utulsa.edu/blog/cybersecurity-defense/ .

5) Tasevski. P, (2015), “Macedonıan Path Towards Cybersecurıty”, Information & Security: An International Journal, available at: https://isij.eu/system/files/download-count/2023-01/3204_macedonia.pdf .

6) The NATO Cooperative Cyber Defense Centre of Excellence, (2018), “Republıc Of Macedonıa Republıc Of Macedonıa Natıonal Cyber Securıty Strategy Securıty Strategy 2018 -2022”, available at: https://ccdcoe.org/uploads/2021/02/North-Macedonia_National-Cyber-Security-Strategy-2018-2022_2018_English.pdf .

7) Kigerl. A, (2011), “Routine Activity Theory and the Determinants of High Cybercrime Countries”, Sage Journals, available at: https://doi.org/10.1177/0894439311422689 .

8) Bruce. M at al, (2024), “Mapping the global geography of cybercrime with the World Cybercrime Index”,Plos One, available at: https://doi.org/10.1371/journal.pone.0297312 .

9) University of Oxford, (2024), “World-first “Cybercrime Index” ranks countries by cybercrime threat level”, available at: https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level .

10) The Official Gazette of R.M no. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 50/2006, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 51/2011, 135/2011, 185/2011, 142/2012, 143/2012, 166/2012, 55/2013, 82/2013.

11) The Official Gazette of R.M no. 150/2010, 100/2012.

12) The Official Gazette of R.M no. 13/2005, 14/2007, 55/2007, 98/2008, 83/2010, 13/2012, 59/2012, 123/2012, 23/2013.

13) The Official Gazette of R.M no. 121/2006, 110/2008, 4/2009, 116/2012.

14) The Official Gazette of R.M no. 133/2007, 17/2011, 188/2014.

15) The Official Gazette of R.M no. 105/2009, 47/2011.

16) The Official Gazette of R.M no. 79/2005, 110/2008, 83/2009, 116/2010.

17) The Official Gazette of R.M no. 34/2001, 98/2008.

18) Metodi Hadji-Janev, (2014), “Toward Effective National Cyber Security Strategy: The Path That Macedonia Must Consider,” available at: http://dx.doi.org/10.3233/978-1-61499-446-6-57 .

19) Council of Europe, (2004), “Convention on Cybercrime (ETS No. 185)”, available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 .

20) European Commission, (2020), “Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse”, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0568 .

21) European Commission, (2019), “Directive on non-cash payment”, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG .

22) European Commission, (2018), “Regulation and Directive facilitating cross-border access to electronic evidence for criminal investigations”, available at: https://home-affairs.ec.europa.eu/error/404_en .

23) European Commission, (2013), “Directive on attacks against information systems”, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF .

24) European Commission, (2011), “Directive on combating the sexual exploitation of children online and child pornography”, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093 .

25) Council of Europe, (2023), “The global state of cybercrime legislation 2013 – 2023: A cursory overview”, available at: https://rm.coe.int/3148-1-3-4-cyberleg-global-state-dec-2023-v4-public/1680adadf0 .