RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0135 • articolo sottoposto a peer review • pubblicato in anteprima il 25 mar. 2024

Vilard Bytyqi

The role of law enforcement agencies in fighting cybercrime in Kosovo: The need to adapt to new trends

Dealing with threats and real risks to cybersecurity that are produced by cybercrime necessarily imposes the construction of a strategic approach at the national and cross-national levels. Despite the fact that Kosovo has built strategies for dealing with cybersecurity, there is still no accurate data regarding the ability of institutional mechanisms to respond in a proportional and effective manner to cybersecurity threats posed by cybercrime. This paper highlights the strategic treatment of cybersecurity and cybercrime, namely the strategic objectives and activities for their fulfillment, as well as critically analyzing the legal rules that are applied in the context of preventing and fighting cybercrime, focusing on the role, responsibilities, and functions of law enforcement agencies for preventing and fighting cybercrime. This paper also analyzes the strategic objectives and the action plan envisaged by the National Cybersecurity Strategy 2023-2027, which for the first time gives special importance to the inclusion of the private sector in the national network to protect against cyber attacks. The importance of the standards of the Budapest Convention is also addressed, and an assessment is made regarding the extent of the inclusion of these standards by the state of Kosovo.

Cybersecurity Strategy – Law Enforcement Agencies – Preventing Cybercrime – Fighting Cybercrime

Il ruolo delle forze dell'ordine nella lotta alla criminalità informatica in Kosovo: la necessità di adattarsi ai nuovi scenari

Affrontare le minacce e i rischi reali per la sicurezza informatica generati dalla criminalità informatica impone necessariamente un approccio strategico a livello nazionale e transnazionale. Nonostante il Kosovo abbia sviluppato strategie per affrontare la sicurezza informatica, non esistono ancora dati accurati sulla capacità dei meccanismi istituzionali di rispondere in modo proporzionale ed efficace alle minacce alla sicurezza informatica poste dalla criminalità informatica. Questo contributo si occupa del trattamento strategico della sicurezza informatica e della criminalità informatica, vale a dire degli obiettivi strategici e delle attività per il loro raggiungimento, e analizza criticamente le norme giuridiche che vengono applicate nel contesto della prevenzione e della lotta alla criminalità informatica, concentrandosi sul ruolo, sulle responsabilità e sulle funzioni delle autorità di contrasto per la prevenzione e la lotta alla criminalità informatica. Nel presente contributo vengono inoltre analizzati gli obiettivi strategici e il piano d'azione previsti dalla Strategia Nazionale di Cybersecurity 2023-2027 che, per la prima volta, attribuisce particolare importanza all'inclusione del settore privato nella rete nazionale per la protezione dagli attacchi informatici. Viene inoltre affrontata l'importanza delle norme della Convenzione di Budapest e viene valutata la portata dell'inclusione di tali norme da parte dello Stato del Kosovo.

Strategia per la cibersicurezza – Autorità di contrasto – Prevenzione della criminalità cibernetica Contrasto alla criminalità cibernetica

The Author is associate professor at the Faculty of Public Safety, at the Kosovo Academy for Public Safety. He is a member of the Kosovo Judicial Council and a trainer at the Academy of Justice

Summary: 1. Introduction. – 2. The Cybersecurity Strategy. – 3. The role of law enforcement agencies in preventing cybercrime. – 4. The role of law enforcement agencies in fighting cybercrime. – 5. The need to adapt to new trends. – 6. Conclusion.

1. Introduction

The approach to cybersecurity, with special emphasis on cybercrime as one of the main cybersecurity threats, requires extensive institutional measures, including clear strategies, appropriate legal rules, clearly defining the roles of institutional mechanisms, and dedicating sufficient resources and professionally prepared officials to meet the objectives for maintaining and advancing cybersecurity.

Concerns about cyber threats have been expressed at various levels: international, regional, and national. This issue has received serious and extensive treatment on the European level, where Kosovo is also a political and geographical part, since cybercrime is considered one of the main issues by the EU authorities in the context of cybersecurity[1]. The treatment of cybercrime at the international level has received a lot of attention when it is known that all countries are affected by this contemporary form of criminality, which is reflected by international initiatives that aim to build a common approach to this form of criminality that is also threatening international security. One of these initiatives is the drafting of the Convention on Cybercrime, which recognizes the need to pursue a common criminal policy as a priority and aims to protect society from cybercrime, among other things, by drafting appropriate legislation and promoting international cooperation in this field[2]. Cybersecurity requires coherent and detailed strategic planning, appropriate legal regulation, and other related measures. Recently, countries around the world have increasingly focused on drafting new laws and other documents, as well as adopting or updating national cybersecurity strategies. Currently, most countries have adopted effective national cybersecurity strategies. The adoption of cybersecurity strategies has been particularly high since 2011[3].

National strategies emphasize the necessity of drafting and effective implementation of legislation in the fight against cybercrime. In this regard, regardless of the design of strategies for cybersecurity and cybercrime or even the design of the criminal legal framework in this area, an important aspect that produces concrete results from the implementation of the law and from the fulfillment of strategic responsibilities remains the role of enforcement agencies of the law, which with their capacities respond to cybersecurity threats. The State Strategy for Cybersecurity is one of the most important documents that deals with cybersecurity and defines the role of law enforcement institutions and agencies in relation to cybersecurity, which is threatened by cybercrime.

This paper first examines the strategic documents and the criminal legal framework for cybersecurity, as well as their compatibility with the standards of international instruments, and shows the need for necessary improvements in the parts where it is estimated that improvements are needed. Then, it examines the need for the design of a new strategy for cybersecurity and analyzes the need that the new strategy must be harmonized

1. Štitilis-Pakutinskas-Malinauskaitė 2017.
2. Council of Europe 2002.
3. Štitilis-Pakutinskas-Laurinaitis-Malinauskaitė 2017, pp. 357-372.

with the standards and guidelines for effective strategies, including, among other things, the need to include the Convention on Cybercrime and other important international instruments in this field. Also, the role, importance, and responsibilities of law enforcement agencies that have a legal mandate to deal with cybercrime prevention and combat are discussed. Among others, the responsibilities of the Information Society Agency, the Kosovo Intelligence Agency, the police, the prosecution, courts, and other law enforcement institutions and agencies are addressed.

2. The Cybersecurity Strategy

Due to the danger posed by cybercrime for internal and international security, this issue is now being dealt with strategically by all countries. This is also observed by international, regional, and global initiatives where the issue of addressing cybercrime is expressed more and more every day. The importance of treating this issue as an area of common international interest is also expressed by the Resolution of the European Parliament of 2013 on the Cybersecurity Strategy of the European Union, where it is emphasized that criminal activities in cyberspace can be equally harmful to the well-being of societies as violations in the physical world and that these forms of crime often reinforce each other, as can be seen, for example, in the sexual exploitation of children, organized crime, and money laundering[4].

Kosovo has drafted and approved the State Strategy for Cybersecurity 2016-2019, becoming one of the first countries in the Western Balkans after Montenegro to draft and approve a strategy in this field[5]. The State Strategy for Cybersecurity has been drafted based on assessments and analyses of the needs of law enforcement agencies, government institutions, local and international organizations, global trends, as well as practices and policies of the European Union. In this context, the strategy is in full harmony with the guidelines of the European Union Agency for Cybersecurity and the strategies of several EU Member States. All state institutions, professional associations, the private sector, civil society, and international partners were included in the working group for the drafting of this document[6].

In terms of structure, this document contains the general principles, legal framework and institutional mechanisms, objectives, system of implementation, monitoring and evaluation of implementation, as well as an action plan. The objectives of the cybersecurity strategy are described in the sixth part of this document and include:

a) protection of critical information infrastructure;
b) development of the institutional and legal framework as well as the development of human and technical capacities;
c) construction of a public-private partnership;
d) reaction to incidents;
e) international cooperation.

The strategy foresees the institutional mechanisms that have a role and importance in cybersecurity and have a mandate for the design and implementation of state policies in this field[7]. This document addresses the responsibilities of institutions and law enforcement agencies in the field of cybercrime and cybersecurity in accordance with their legal mandate and foresees that this strategy has the coordination of the Ministry of Internal Affairs or one of his authorized representatives. In this regard, some states are now re-examining the issue of policy formulation and implementation at a higher state and more professional level; e.g., Germany, Japan and the Netherlands plan a strategic-level cybersecurity council[8].

In this strategy, dealing with cybercrime does not receive much attention, as the entire focus of this document is on strengthening capacities for cybersecurity. Cybercrime draws attention to the part of the legal infrastructure where it is foreseen

4. Joint communication to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Cyber security strategy of the European Union: an open, safe and secure cyberspace*, JOIN/2013/01, Brussels 7 February 2013.
5. Kosovar Center for Security Studies 2022.
6. Ministry of Internal Affairs 2015.
7. *Ibid*.
8. Luiijf-Besseling-Spoelstra-De Graaf 2013.

that the law on the prevention and combating of cybercrime should be reviewed based on modern trends to respond to this form of crime. Meanwhile, special care has been devoted to the advancement of the technical infrastructure with the aim of advancing the equipment for the investigation of cybercrime[9]. In the same way as Kosovo, the national cybersecurity strategies of many countries do not directly mention the fight against cybercrime or reducing the number of cybercrimes. However, there are also countries that reserve a separate chapter for the treatment of cybercrime[10]. Even in the document published by the Global Cybersecurity Capacity Center[11], it is emphasized that Kosovo still does not have any cybersecurity command and control centers at the national level. Although the Kosovo Security Force and Police have cybercrime units, their capacities are severely limited due to a lack of human resources.

Even though this document is intended to revise the Law on the Prevention and Fight Against Cybercrime, this process has never been completed, which is why the legal rules applicable to the prevention and fight against cybercrime have not been updated and adapted to the trends of cybercrime, which, as a form of crime, stands out for the fast dynamics of its development. The field of cybernetics is regulated by several legal acts that are approved by the Assembly of Kosovo, including here, *Law on Information Society Government Bodies*[12]; *Law on the Information Society Services*;[13] *Law on Electronic Communications*[14]; *Law on Interception of Electronic Communications*[15]; as well as the *Law on Protection of Personal Data*[16].

3. The role of law enforcement agencies in preventing cybercrime

Building a proper approach to cybercrime prevention is a rather complex issue. In addition to the general approach to crime prevention that is known in the theories of crime prevention, in the cybercrime prevention strategy, some other approaches are also used that adapt to the specifics that characterize this particular form of criminality. In this regard, genuine criminal investigations allow us to understand the modus operandi used by persons involved in cybercrime as perpetrators of criminal offences. A broad understanding of modus operandi can be used by law enforcement agency officials to design and implement cybercrime prevention policies. Also, intelligence and strategic analysis are vital in the fight against cybercrime. Europol recently adopted a very well-structured strategic analysis methodology in the framework of Serious and Organized Crime Threat Assessment (SOCTA). Such a methodology, generally built to analyze the threat posed by serious organized groups, can be used, mutatis mutandis, to examine the specifics of cybercrime threats[17].

Based on the legal and strategic framework applicable in Kosovo, in the following we will reflect on the institutions and law enforcement agencies that have in their scope the prevention of crime, including cybercrime.

At the strategic level, the Ministry of Internal Affairs is the central authority that coordinates activities with all institutions and law enforcement agencies in the field of cybersecurity and has the obligation to monitor the implementation of the strategy and the fulfillment of strategic objectives.

9. Ministry of Internal Affairs 2015.
10. Štitilis-Pakutinskas-Malinauskaitė 2017.
11. Bada 2015.
12. *Law on Information Society Government Bodies*, Official Gazette of the Republic of Kosovo, No. 15/2013, 15 May 2013, Law No. 04/L-145.
13. *Law on the Information Society Services*, Official Gazette of the Republic of Kosovo, No. 6/2012, 11 April 2012, Law No. 04/L-094.
14. *Law on Electronic Communications*, Official Gazette of the Republic of Kosovo, No. 30/2012, 9 November 2012, Law No. 04/L-109.
15. *Law on Interception of Electronic Communications*, Official Gazette of the Republic of Kosovo, No. 18/2015, 13 July 2015, Law No. 05/L-030.
16. *Law on Protection of Personal Data*, Official Gazette of the Republic of Kosovo, No. 6/2019, 25 February 2019, Law No. 06/L-082.
17. Buono 2014.

For this purpose, at the level of this institution, the Secretariat of Strategies functions as a permanent body that has a mandate for all strategic documents issued by the Government of Kosovo. The Information Society Agency was established by the Law on Information Society Government Bodies and serves as the central body of the state administration for the development and implementation of information and communication technology for the institutions of the Republic of Kosovo (Article 5)[18]. Also, as needed, the Information Society Agency helps the relevant institutions in the fight against cybercrime and ensures the protection of personal data in electronic form in accordance with the legislation in force[19].

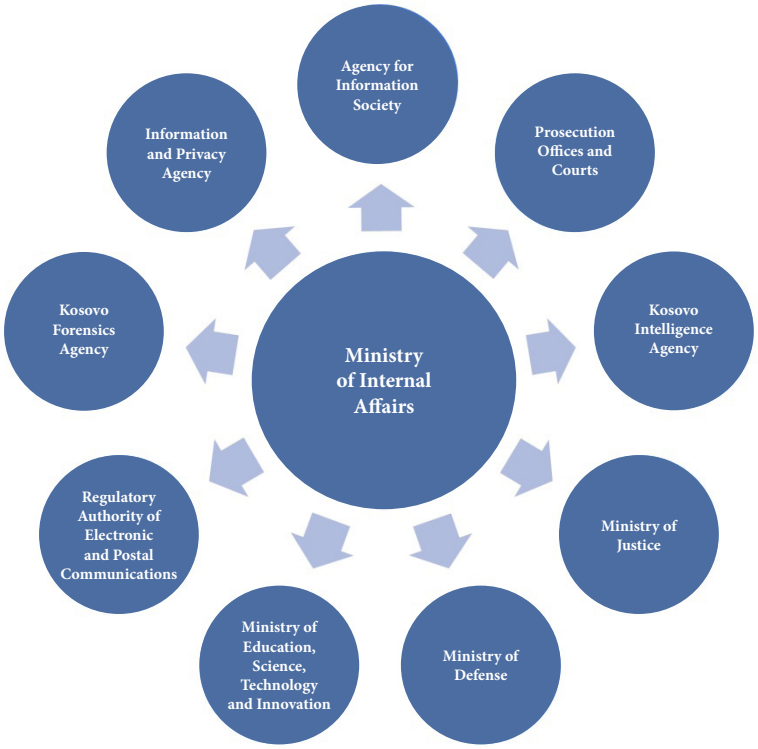

Fig. 1 — *Institutions and law enforcement agencies that have a mandate to prevent cybercrime* [Ministry of Internal Affairs 2023]

An important function for the identification and detection of potential threats that endanger cybersecurity is also played by the Kosovo Intelligence Agency, which, within its constitutional and legal mandate, has the authority to collect information about threats to the security of Kosovo, which includes the collection of intelligence information for the purposes of cybersecurity protection[20]. The role of the Kosovo Intelligence Agency as a national security institution is not clearly defined by the State Strategy for Cybersecurity 2016-2019. In addition to the activity that is foreseen by the Action Plan of this strategy for the advancement of regional and international cooperation in the fight against cybercrime that is determined to be fulfilled together with some other law enforcement authorities, the specific tasks related to the fulfillment of any specific task are not highlighted in this document; therefore, the commitment of the Kosovo Intelligence Agency remains unclear for the implementation of this strategy.

On the other hand, the police, as an agency within the Ministry of Internal Affairs, play an important role in preventing crime in general, including taking measures to prevent cybercrime. This duty is provided in Article 10 of the *Law on Police*[21], as one of the general duties of the police, which, among other things, provides for the prevention of danger to citizens and to maintain order and public safety, as well as to prevent and detect criminal offences and their perpetrators, including taking proactive actions to prevent cybercrime.

To fulfill its legal mandate, the issue of police crime control involving digital technology and

18. *Law on Information Society Government Bodies*, Official Gazette of the Republic of Kosovo, No. 15/2013, 15 May 2013, Law No. 04/L-145.
19. Ministry of Internal Affairs 2015.
20. *Law on the Kosovo Intelligence Agency*, Official Gazette of the Republic of Kosovo, No. 30/2008, 15 June 2008, Law No. 03/L-063.
21. *Law on Police*, Official Gazette of the Republic of Kosovo No. 4/2012, 19 March 2012, Law No. 04/L-076.

computer networks also requires a range of new collaborations, including collaboration between the police and other agencies, collaboration between the police and private institutions, and collaboration between the police of at least two states, namely the creation and advancement of international cooperation, which can be done through permanent mechanisms that have already been established or even through direct relations between the police[22]. Considerable progress has been made over a period of time in building the capacity of the national police to respond to cybercrime, and there is now a growing awareness among computer users of the need for basic Internet security[23].

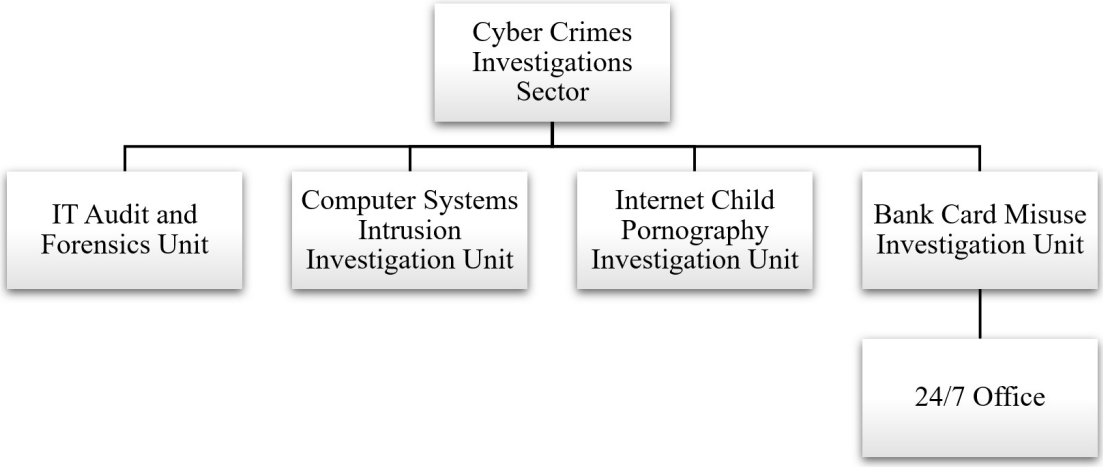

Fig. 2 — *The organizational structure of the Cybercrime Investigations Sector* [Kosovo Police 2019]

An important role in the prevention of cybercrime in the institutional structure is also exercised by other institutional mechanisms which are defined according to the Law on Electronic Communications, Law on Protection of Personal Data, as well as other laws.

4. The role of law enforcement agencies in fighting cybercrime

Depending on national specifics, states are organized differently to investigate and prosecute cybercrime; e.g., the United Kingdom, due to the specifics of its internal organization, addresses the issue of investigation and criminal prosecution through many central and local institutional mechanisms that are specialized in dealing with cybercrime[24]. In many countries around the world, law enforcement agencies have developed specialized units[25]. While in Kosovo, the primary responsibility for the investigation and documentation of criminal offences in the field of cybernetics is with the police, other law enforcement agencies are involved in the investigation of these criminal offences when it is necessary to build joint investigative groups or the criminal case falls directly under the legal responsibilities that these agencies have. The concentration of resources in only one agency is due to the possibility of more effective criminal investigation and prosecution, but also due to the low rate of presentation of criminal offences for which the state must have the capacity to respond. Focusing only on one state agency for the investigation of these crimes can be found in many small countries; e.g., Iceland is one such example where the criminal investigation is concentrated only in the capital[26].

In Kosovo, the procedure for investigating criminal offences is regulated according to the

22. Broadhurst 2006.
23. *Ibid.*
24. Bada-Arreguin-Toft-Brown et al. 2016.
25. Brown 2015.
26. Bada-Arreguin-Toft-Brown et al. 2016.

Code of Criminal Procedure, where it is determined that initial police actions are the responsibility of law enforcement agencies that have police

Agency	Law	Scope
The Tax Administration of Kosovo	Law No. 03/L-222 on Tax Administration and Procedures	Art. 75 (1)
Customs	Code No. 03/L-109 Customs and Excise Code of Kosovo	Art. 302 (1)
Police Inspectorate of Kosovo	Law No. 03/L-23 on Police Inspectorate of Kosovo	Art. 2 (1) (1)
Financial Intelligence Unit of the Republic of Kosovo	Law No. 05/L-096 on the Prevention of Money Laundering and Combating Terrorist Financing	Art. 4 (1)

Tab. 1 — *Law enforcement agencies that have police powers in Kosovo*

authorizations[27]. The Code of Criminal Procedure does not explicitly define the law enforcement agencies that have police powers, as this issue is dealt with by separate laws that regulate the scope of these agencies. According to special laws, in addition to the police, there are also several other law enforcement agencies that have police authorizations, listed in table 1.

These agencies can act independently when the criminal investigation of cybercrime cases is within their mandate defined by law and does not relate to the scope of other law enforcement agencies. These law enforcement agencies operate under the authority of the State Prosecutor.

Depending on the scope and complexity of the crime, several law enforcement agencies may jointly investigate a complex criminal case, including cybercrime. The joint investigation comes into expression even when cybercrime has such an extent that it violates the laws of at least two countries, which has international elements, and there is a need to develop joint procedures for the investigation of these criminal offences. This activity can be facilitated by international instruments for international legal cooperation as well as direct agreements concluded between states. The traditional mechanisms of criminal investigation and prosecution have been assessed as insufficient to combat serious cross-border crime, including cybercrime that operates in a virtual world with the possibility of taking actions and causing consequences in an unpredictable manner. Therefore, it has been estimated that the creation of a joint team of two or more states would effectively improve crime with an international element. Investigations would be coordinated, while prosecutors would directly access relevant information from different countries[28].

Within the police organization, the Department of Investigation functions as one of the three main pillars that make up the high structure of the internal organization of this agency[29]. This pillar also deals with the aspect of criminal offences in the field of cybernetics since the Directorate Against Organized Crime functions as a separate unit within its hierarchy and has the Cybercrime Investigation Sector. The scope of this unit is related to serious criminal offences for which in-depth investigation and special expertise are required, since other criminal offences from the field of cybernetics can also be investigated by non-specialized units that operate within the police stations that deal with crime generally.

27. *Criminal Procedure Code*, Official Gazette of the Republic of Kosovo, No. 24/2022, 17 August 2022, Code No. 08/L-032.
28. Deutsche Gesellschaft für Internationale Zusammenarbeit 2014.
29. *Law on Police*, Official Gazette of the Republic of Kosovo No. 4/2012, 19 March 2012, Law No. 04/L-076.

According to the organizational structure, five units operate in the Cybercrime Investigation Sector, namely the IT Control and Forensics Unit, the Computer Systems Intrusion Investigation Unit, the Internet Child Pornography Investigation Unit, the Card Abuse Investigation Unit, and Banking and Office 24/7[30]. The 24/7 Office is a mechanism envisaged by the Convention on Cybercrime of the Council of Europe as a point of contact available twenty-four hours a day, seven days a week, in order to ensure the provision of immediate assistance for the purposes of investigations or procedures related to criminal offences related to computer systems and data or to the collection of evidence in electronic form related to the criminal offence. The Convention on Cybercrime provides for the 24/7 clause to expedite and, in some cases, act as competent authority when urgent action is required on certain issues[31]. Precisely for this purpose, the 24/7 Office that operates within the Cybercrime Investigations Sector aims to play the role that the Convention on Cybercrime provides for quick actions related to cybercrime issues or other issues related to this field.

In the fight against cybercrime, the police is challenged by many issues, especially: number of users, the availability of tools and information, difficulties in tracing offenders, missing mechanisms of control, the absence of borders in cyberspace and the international component of cybercrime. Not only is the complexity of investigating cybercrimes, but cyber policing in general tends to be hampered. It is very difficult for police units to initiate investigations due to the invisibility of such crimes and lack of reporting[32].

The State Prosecutor is responsible for the prosecution of persons suspected of these criminal offences[33]. The State Prosecutor still does not have any special units or specialized prosecutors that would specifically deal with the prosecution of these criminal offences. Also, the courts do not have any special departments that judge criminal offences in this field. All courts of first instance have the competence to deal with these criminal offences, as provided by the Law on Courts[34]. Also at the appeal level, the judicial system does not have any specialized department that will deal with this category of criminal offences. In addition to the lack of specialization at the institutional level, there is also a lack of specialization among judges, since they deal with all criminal cases that fall under the competence of the department where they serve. The importance of the specialization of courts and judges for specific cases, including the field of cybercrimes, is manifold, since the judges who deal with these cases have relevant professional expertise, but the courts are also more efficient[35].

Although there are no prosecutors and judges who will deal only with these criminal offences, specialized trainings related to the field of cybercrime are organized. This is also reflected in the annual programs organized by the Academy of Law, where cybercrime training is foreseen, namely several training sessions for judges and prosecutors who deal with cybercrime issues[36].

5. The need to adapt to new trends

Even though the duration of the State Strategy for Cybersecurity was valid only for the period 2016–2019, the document for the new strategy is in the drafting phase by the Ministry of Internal Affairs and is now open to public consultation. The lack of a workable document that deals with cybersecurity from a strategic point of view has created a vacuum for dealing with the problem from a strategic perspective, even worse when it is known that a front of multi-disciplinary mechanisms must be built to approach the problem of cybercrime and cybersecurity, which is now one of the most serious threats to not only national but also international security. The national cybersecurity strategy, as a strategic document, should be one of the es-

30. *Ibid.*
31. Council of Europe 2002.
32. Tropina 2017.
33. Sahiti-Murati-Elshani 2014.
34. *Law on Courts*, Official Gazette of the Republic of Kosovo, No. 22/2018, 18 December 2018, Law No. 06/L–054.
35. Wasserman-Slack 2021.
36. Academy of Justice 2023.

sential documents in every state that provides the basics and measures to guarantee cybersecurity, as well as the priorities for its improvement[37].

The importance of dealing with this issue in a strategic aspect is proven by the treatment of cybercrime and cybersecurity in the Security Strategy of Kosovo, where cybercrime and cybersecurity are identified as issues that constitute one of the challenges that the global security environment faces today, where Kosovo is also exposed to hybrid threats, which include non-conventional, foreseen with the Security Strategy and Cybersecurity Strategy (2016-2019) were insufficient to include the private sector, which is one of the most sensitive areas exposed to threats from cybercrime. In the National Cybersecurity Strategy 2023-2027, for the first time as a special objective, «Advancement of investigative and military cybersecurity capabilities» is envisaged. One of the concrete measures related to the fulfillment of this objective is the advancement of legislation; collecting accurate and reliable statistics; increasing the number

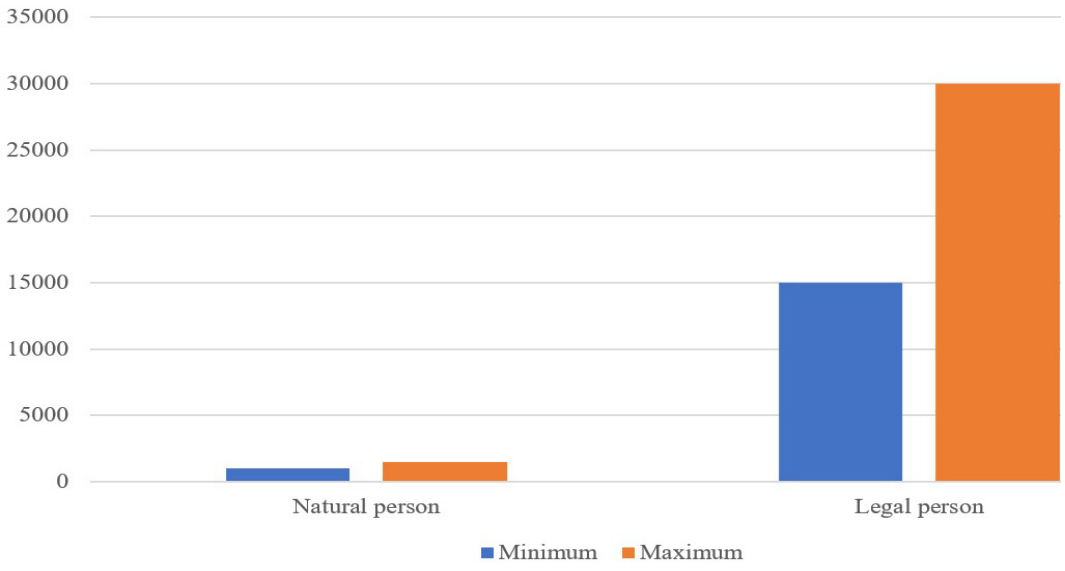

Fig. 3 — *Minor offence sanctions*

asymmetric elements that influence extension operations and cyber attacks that aim to weaken the country's sovereignty, undermine the country's integrity, and damage the country's image in the international arena[38].

National Cybersecurity Strategy 2023-2027 presents a more advanced document that includes the most important aspects that a strategic document should contain. Unlike the previous strategy, this document contains aspects that are addressed for the first time, with special emphasis on the treatment and protection from cyber threats of the non-state sector as well. Such a strategic approach fills the former and current vacuum on this issue. The strategic institutional mechanisms that were of law enforcement officials in the police, prosecutor's office, and courts; and engaging experts from the private sector. The activities planned for this strategic objective will be classified and not made public.[39]

At the international level, guidelines have already been drawn up for the drafting of these strategic documents that will help the states build effective strategies at the domestic level. One of them is the Guide to Developing a National Cybersecurity Strategy, where this document provides some good practices that states should adapt in their national documents, including governance, risk management in national cybersecurity, preparedness and resilience, critical infrastructure services and

37. Štitilis-Pakutinskas-Laurinaitis-Malinauskaitė 2017.
38. Government of Kosovo 2022.
39. Ministry of Internal Affairs 2023.

essential services, capability and capacity building and awareness raising, legislation and regulation, and international cooperation.[40]

In addition to addressing cybercrime and cybersecurity in terms of strategic documents, a number of legal initiatives have been undertaken to address cybercrime and cybersecurity. One of them is the initiative of the government to sponsor the Law on Cybersecurity, which has already passed the institutional filters, starting from the Ministry of Internal Affairs and the government, and has been approved by the Assembly of Kosovo. This law defines the principles of cybersecurity, the institutions and agencies that develop and implement the cybersecurity policy, the responsibilities of the authorities in the field of cybersecurity, the duties of cybersecurity entities, inter-institutional cooperation, as well as the prevention of cyber attacks in the Republic of Kosovo. With this law, the Cybersecurity Agency is established for the first time[41]. The Agency for Cybersecurity will have primary responsibility for the implementation of this law and will act under the authority of the Ministry of Internal Affairs. It will also have the authority to coordinate activities relevant to the fulfillment of the cybersecurity mission with all parties involved in cybersecurity, inside and outside Kosovo.

In this law, it is foreseen that in some parts the Law on Prevention and Fight of Cybercrime[42] will be supplemented or amended, as it is planned that some legal provisions of this law will be repealed, namely Article 5 in its entirety (prevention, security, and informative campaigns), Article 6 (maintenance, completion, and use of the database), Article 7 (training and special programs), and Article 8 (obligations of owners and administrators)[43]. This law partially transposes Directive 2013/40/EU[44] of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, as well as Directive (EU) 2016/1148[45] of 6 July 2016 concerning measures for a high common level of security of networks and information systems across the Union.

According to Article 3 of the law, the expressions "operator of essential services" and "provider of digital services" are defined. According to the law, the expression "operator of essential services" means a public or private entity that possesses national critical infrastructure according to the respective Law on Critical Infrastructure (Art. 3 (1)(12)). While the expression "Digital service provider" means a legal person with a base or branch registered in the Republic of Kosovo that provides digital services (Art. 3 (1)(13)). This definition is harmonized with points (4) and (6) of Article 4 of Directive (EU) 2016/1148.

The law provides a separate chapter for obligations to guarantee cybersecurity. In this regard, the operator of essential services must permanently implement organizational security measures as well as determine if any cyber incident has occurred that has a significant impact on system security or service continuity (Article 5 and Article 6)[46]. Also, the provider of digital services is required to ascertain the risks that affect the security of their system, analyze them, and take adequate organizational and technical measures for risk management. The digital service provider must notify the Cybersecurity Agency of a cyber incident that has a significant impact on the digital service provided immediately after becoming aware of the cyber incident (Article 7 and Article 8). The law foresees

40. International Telecommunication Union 2018.
41. *Law on Cybersecurity*, Official Gazette of the Republic of Kosovo, No. 4/2023, 22 February 2023, Law No. 08/L-173.
42. *Law on Prevention and Fight of the Cyber Crime*, Official Gazette of the Republic of Kosovo, No. 74/2010, 20 July 2010, Law No. 03/L-166.
43. L*aw on Cybersecurity*, Official Gazette of the Republic of Kosovo, No. 4/2023, 22 February 2023, Law No. 08/L-173.
44. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
45. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
46. *Law on Cybersecurity*, Official Gazette of the Republic of Kosovo, No. 4/2023, 22 February 2023, Law No. 08/L-73.

the possibility of imposing criminal sanctions if it is estimated that operators of essential services and providers of digital services do not take the measures defined in Articles 5, 6, 7, and 8 of this law[47]. The law foresees the possibility of imposing criminal sanctions (fines) against legal persons and natural persons.

The Law on Cybersecurity foresees minor offence sanctions, namely higher fines for legal entities while lower fines are provided for natural persons. This law does not foresee any criminal offence for violating its legal provisions. In this regard, this law only provides for minor offence sanctions that are imposed in administrative procedure by the relevant authorities.

Despite the effort to advance the regulation of this field with effective laws, there is still a lack of concrete implementation of the provisions contained in the Convention on Cybercrime, known as the Budapest Convention. The primary purpose of this instrument is to advance and fulfill the objectives for preventing and fighting cybercrime at the national level, with the aim of producing results at the international level as well. This is also reflected in the goals of this instrument, which can be summarized as follows: 1) harmonization of domestic material criminal laws in the field of cybercrime; 2) ensuring the necessary legal powers of the criminal procedure for the investigation and prosecution of such crimes; and 3) creating a fast and effective international cooperation mechanism[48].

The Convention on Cybercrime aimed to establish an important basis of cooperation between states, creating an important reference in terms of content, but it also aimed to unify the rules between states, which is reflected in the fact that this instrument, although it was sponsored by the Council of Europe, remains open for ratification by other countries that are not members of this international organization. This is proven by the large number of countries that are not members of the Council of Europe; an example is the USA, but there are also other countries. Now this instrument has 67 party states, of which 1 third are not members of the Council of Europe.

6. Conclusion

The State Strategy for Cybersecurity is one of the most important documents that deals with cybersecurity and defines the role of law enforcement institutions and agencies in relation to cybersecurity, which is threatened by cybercrime. The State Strategy for Cybersecurity of Kosovo was one of the first documents approved in this field in the Western Balkans. The strategy foresees the institutional mechanisms that have a role and importance in cybersecurity, and these institutional mechanisms have a mandate for the design and implementation of state policies in this field. In the strategy implemented during the period 2016-2019, the treatment of cybercrime does not receive much attention, as the focus is on strengthening capacities for cybersecurity.

A number of important legal initiatives have been undertaken that focus on dealing with cybersecurity and cybercrime. One of these initiatives is the government's initiative to sponsor the Law on Cybersecurity, which has already passed the institutional filters and been approved by the Assembly of Kosovo. The field of cybernetics is regulated by several legal acts issued by the Assembly of Kosovo, including the Law on Information Society Government Bodies, the Law on Information Society Services, the Law on Electronic Communications, the Law on Interception of Electronic Communications, and the Law on Protection of Personal Data. Regarding the functions performed by law enforcement agencies for the prevention and combating of cybercrime, there is no special treatment from a strategic point of view, even though this part is very important and stands out from many international instruments in this field.

Regarding the fight against cybercrime, the police have the primary responsibility for investigating and documenting criminal offences in the field of cybernetics, while other law enforcement agencies are involved in the investigation of cybercrime when necessary. The procedure for the investigation of criminal offences is regulated according to the Code of Criminal Procedure, which states that initial police actions are the responsibility of law enforcement agencies that have police authorizations.

47. *Ibid.*
48. Brenner 2007.

Within the police, there is a special unit that deals with cybercrime, while the prosecution and courts do not have any specialized departments that specifically deal with this category of criminal offences.

National Cybersecurity Strategy 2023-2027 presents an advanced document that includes the most important components that a strategic document should contain. This document is the continuation of the previous strategy in this area. Unlike the previous strategy, this document is more advanced and contains components that are included for the first time, with special emphasis on the treatment and protection from cyber threats of the non-state sector as well. The issue of cybercrime investigations is also dealt with in detail and is detailed in an important way in the action plan of this document. Despite the advancement of the strategic and legal framework in the field of cybersecurity and cybercrime, the full transposition of the rules and standards contained in the Budapest Convention has not yet been done.

References

Academy of Justice (2023), *Training Program 2023*, Prishtina, 2023

M. Bada (2015), *Cyber security Capacity Assessment of the Republic of Kosovo*, Global Cyber Security Capacity Centre, 2015

M. Bada, I. Arreguin-Toft, I. Brown et al. (2016), *Cyber security Capacity Review of the United Kingdom*, Global Cyber Security Capacity Centre, University of Oxford, 2016

S.W. Brenner (2007), *Cybercrime: Re-Thinking Crime Control Strategies*, in Y. Jewkes (ed.), "Crime Online", Willan, 2007

R. Broadhurst (2006), *Developments in the global law enforcement of cyber-crime*, in "Policing: An International Journal", vol. 29, 2006, n. 3

C.S.D. Brown (2015), *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, in "International Journal of Cyber Criminology", vol. 9, 2015, n. 1

L. Buono (2014), *Fighting cybercrime through prevention, outreach and awareness raising*, in "ERA Forum. Journal of the Academy of European Law", vol. 15, 2014, n. 3

Council of Europe (2002), *Convention on Cybercrime,* Budapest, 23 November 2001, Council of Europe Publishing, 2002

Deutsche Gesellschaft für Internationale Zusammenarbeit, *The fight against organized crime and corruption: Strengthening the Network of Prosecutors*, Sarajevo, 2014

Government of Kosovo (2022), *Kosovo Security Strategy 2022-2027*, Prishtina, 2022

Kosovar Center for Security Studies (2022), *Safeguarding Critical Infrastructure in Kosovo. Deconstructing Existing Policies and Practice*, Prishtina, 2022

Kosovo Police (2019), *The organizational structure of the Cybercrime Investigations Sector*, Pristina, 2019

International Telecommunication Union (2018), *Guide to Developing a National Cyber security Strategy. Strategic Engagement in Cyber security*, ITU, 2018

H.A.M. Luiijf, K. Besseling, M. Spoelstra, P. De Graaf (2013), *Ten National Cyber Security Strategies: a Comparison: Critical Information Infrastructure Security*, in S. Bologna, B. Hämmerli, D. Gritzalis, S. Wolthusen (eds.), "Critical Information Infrastructure Security", Springer, 2013

Ministry of Internal Affairs (2023), *National Cyber Security Strategy 2023-2027*, Pristina, 2023

Ministry of Internal Affairs (2015), *National Cyber Security Strategy and Action Plan 2016-2019*, 2015

E. Sahiti, R. Murati, XH. Elshani (2014), *Commentary - The Code of the Criminal Procedure*, Pristina, 2014

D. Štitilis, P. Pakutinskas, M. Laurinaitis, I. Malinauskaitė (2017), *A Model for the national cyber security strategy. The Lithuanian case*, in "Journal of security and sustainability issues", vol. 6, 2017, n. 3

D. Štitilis, P. Pakutinskas, I. Malinauskaitė (2017), *EU and NATO cyber security strategies and national cyber security strategies: a comparative analysis*, in "Security Journal", vol. 30, 2017

T. Tropina (2017), *Cyber-policing: the role of the police in fighting cybercrime*, in "European Law Enforcement Research Bulletin", 2017, n. 2

M.F. Wasserman, J.D. Slack (2021), *Can There Be Too Much Specialization? Specialization in Specialized Courts*, in "Northwestern University Law Review", vol. 115, 2021, n. 5