Expanding the Potential of the Preventive and Law Enforcement Function of the Security Police in Combating Cybercrime in Ukraine and the EU

Igor Kopotun [1], Anatolii Nikitin [2], Nataliia Dombrovan [2], Valentyn Tulinov [3], Dmytro Kyslenko [4]

[1]Academy Huspol, 381 Rybářská, Hranice, 753 61, Czech Republic
[2] Odesa State University of Internal Affairs, 1 Uspenska str., Odesa, 65014, Ukraine
[3] Donetsk Law Institute of Ministry of Internal Affairs of Ukraine, Kryvyi Rih, 50065, Ukraine
[4] National University of Ukraine on Physical Education and Sport, 1 Phizkultury str., Kyiv, 03150, Ukraine

***Abstract* – The research paper deals with the search for practical means of enhancing the functional and organizational capabilities of the security police in combating cybercrime. The research paper separately examines the influence of municipal security police on the cybercrime combating system. It also reveals the interaction of the municipal police with the system of national police authorities. The conclusion is that there is a need to introduce municipal security police in Ukraine to increase the flexibility and mobility of law enforcement agencies in responding to cybercrime, and to enhance the level of protection of municipal property that may be targeted by cybercrimes.**

***Keywords* – cybercrime, security police, municipal security police, preventive function, counteraction to cybercrime.**

DOI: 10.18421/TEM92-06
https://doi.org/10.18421/TEM92-06

Corresponding author: Dmytro Kyslenko,
National University of Ukraine on Physical Education and Sport, 1 Phizkultury str., Kyiv, 03150, Ukraine
Email: dmytro.kyslenko39@gmail.com

Received: 16 January 2020.
Revised: 26 March 2020.
Accepted: 02 April 2020.
Published: 27 May 2020.

1. Introduction

In modern democratic countries, the police institution is one of the most important manifestations of state monopoly on the use of legal coercion. Maintaining public order, ensuring public safety and combating crime are the tasks that are legally fulfilled solely by law enforcement agencies, with the crucial and the leading role assigned to the police authorities. Police authorities are not, however, monolithic, and the police institution itself can bring together a large number of authorities and institutions with similar function, uniform and subordination, but different powers and overseeing different spheres of public relations. One of the elements of the system of police authorities is the security police, which have a special purpose in terms of meeting the needs for quality protection of different entities and individuals, not only the public sector but also the private sector. Although, the effectiveness of the security function of police is gradually diminishing, while increasing the importance of preventive function. The topicality of this function is especially manifested in the context of combating cybercrime, as the search for traces of committing such crimes is becoming increasingly difficult due to the increasing level of professional qualification of criminal elements. Thus, we suggested the main hypothesis of this study: the potential of security police should be used to combat cybercrime, that is, not only the security function, but also the preventive one. This hypothesis implies the achievement of the following research objectives:

- identifying legislative opportunities for extending law enforcement powers of security police in the context of preventing and combating cybercrime;

- determining mechanisms for expanding functional tools for security police in Ukraine and across the EU in the context of counteraction to cybercrime;
- identifying subject areas of cybercrime that can be covered by the preventive and security functions of the security police.

2. Methods and Materials

The study is based on a sufficiently extensive regulatory framework, which primarily consists of regulatory acts of both the EU and individual countries, including the legislative acts of Ukraine.

In particular, the 2001 Convention on Cybercrime, Directive (EU) 2016/1148, Directive (EU) 2019/713, Directive 2000/31/EC, Directive 2011/93/EU, Directive 2013/40/EU and other legislative acts, including those of the EU Member States, in particular the 2017 Policing and Crime Act, etc. were used. Among the legal acts of Ukraine, we studied the Laws of Ukraine “On the National Police”, “On Security Activities”, as well as the Cabinet of Ministers of Ukraine Decrees No. 975 and No. 421.

The opportunities of expanding the legal status of the police authorities in Ukraine in the field of combating cybercrime were analysed based on [1], [2] and others. The analysis of the European experience in the management and organization of the activities of police authorities and the possibility of its use in Ukraine was based on [3], [4], [5] and others.

The opportunities of using the police authorities in combating cybercrime and minimizing cybercrime in EU countries were analysed based on [6], [7], [8] and others. When studying the possibility of using municipal security police in combating cybercrime, we considered [9], [10], [11] and others mandatory for the analysis.

The research methodology was as follows: at the first stage, we examined the EU and the Ukrainian legislation in the field of security police using systemic method and method of structural analysis; the second stage was an analysis of the functional burden on the security police in the context of combating cybercrime. The question was whether and how the security police are involved in combating cybercrime. At the third stage, formal and logical, as well as dialectical analysis was used to find ways to expand the functions and change the paradigm of the security police as a separate element of the national law enforcement systems in the EU countries. Finally, at the last stage of the study, possible models and forms of involvement of the security police in the process of counteraction to cybercrime were identified through legal modelling methods.

3. Results

Cybercrime as a type of illegal activity is a fairly new phenomenon in the forensic and criminological fields, but it is the fastest developing and improving kind of criminal activity. In 2001, the Council of Europe adopted the so-called Budapest Convention on Cybercrime, where the most important achievement is the classification of cybercrimes [12]. Analysing the provisions of the Convention on Cybercrime (the Budapest Convention), it should be noted that the Council of Europe helps to protect European societies from the threat of cybercrime through this Convention and its Protocol on Xenophobia and Racism (with the participation of the Cybercrime Convention Committee, T-CY) and cybercrime technical cooperation programs (C-PROC) (Figure 1).

The institutional component of counteracting cybercrime in the EU countries is primarily realized in the activities of Eurojust (Agency of the European Union (EU) for dealing with judicial co-operation in criminal matters among member state agencies). In the analysed segment of law enforcement, Eurojust’s powers include both opening of criminal investigations into cybercrime and the recommendations to national law enforcement agencies to open them. In 2013, a separate special body is set up in the EU – the European Cybercrime Centre, which aims at collecting and processing cybercrime data, conducting expert assessments of cybercrime, developing and implementing advanced methods of cybercrime prevention and investigation, etc. [2], [7].

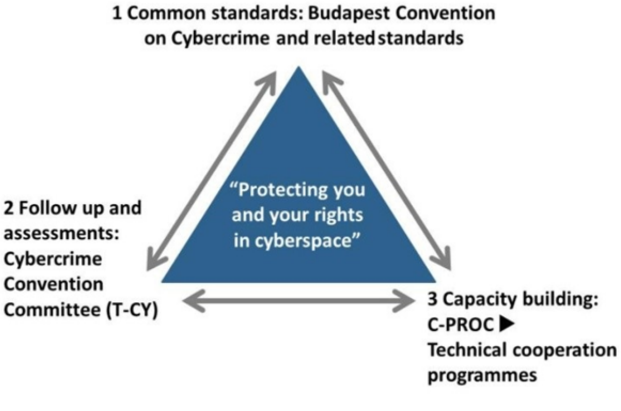
1 Common standards: Budapest Convention on Cybercrime and related standards
“Protecting you and your rights in cyberspace”
2 Follow up and assessments: Cybercrime Convention Committee (T-CY)
3 Capacity building: C-PROC ▶ Technical cooperation programmes

Figure 1. Cybercrime counteraction mechanism at the EU level

Thus, it can be argued today that the system of special law enforcement agencies for combating cybercrime in the EU has the following institutional component, taking into account the national law enforcement agencies in this field (Table 1).

Table 1. Institutional elements of the cybercrime counteraction system in the EU, some EU Member States and Ukraine [based on [7] and [12]

Country	**Membership in the Convention on Cybercrime**	**Extending the jurisdiction of EU cybercrime authorities**	**National cybercrime authorities**
EU	being adopted	Eurojust; European Cybercrime Centre	
United Kingdom	yes	European Cybercrime Centre only	Electronic Communication Security Group of the Ministry of Foreign Affairs; the Defence Ministry's Virtual Threat Protection Unit
Germany	yes	both authorities	Special group at the Ministry of Internal Affairs of Germany
France	yes	both authorities	Separate unit of the National Gendarmerie
Ukraine	yes	no	Cyber police of the Ministry of Internal Affairs of Ukraine

An important step towards solving the problems set out in the research paper is to identify the legislative framework for the security police in Ukraine and the EU countries, as well as the possibilities of expanding their functions and subject areas of operation, where the analysis of the legislation will be helpful. According to the Law of Ukraine "On National Police", the National Police of Ukraine (Police) is the central executive body that serves the society by ensuring the protection of human rights and freedoms, combating crime, maintaining public safety and order. It includes: the criminal police; patrol police; pre-trial investigation bodies; security police; special police; Operative-Sudden Action Corps. According to the Law of Ukraine "On Security Activities", security activities are the provisions of services for protection of property and citizens. The following types of security services are determined: protection of the property of citizens; protection of the property of legal entities; protection of individuals. In Ukraine, security can be ensured not only by the police, although it is clearly the most effective entity in the security market. In addition, the monopoly position of the security police as an entity providing security services or an entity performing a security function is also determined by Decrees of the Cabinet of Ministers of Ukraine No. 975 and No. 421.

The Ukrainian security services segment is characterized by high concentration and dominance by the government. Although the number of companies in this segment has increased in recent years, several large companies still dominate. These companies are mainly concentrated in Kyiv and represent only 15% of the total number of market participants, but they control 80% of the market. The government entity – security police – which is one of these large organizations, controls about 30% of the market, making it the largest player. At the same time, as indicated in the Special Report of the Commercial Service of the US Embassy in Ukraine, the involvement of security market actors in the protection of cyber objects and computer networks is extremely low. The security police provide physical protection of only the server facilities and wired nodes of the state-owned computer and telecommunication networks. The security police are less often involved in the physical protection of the respective objects of commercial private banks [13]. There is no other involvement of the police in the field of prevention of and counteraction to cybercrime.

With regard to the security police agencies of the EU member states, it should be noted that, in general, law enforcement activities in the field of combating and preventing cybercrime are based on the following acts of the EU, in addition to the Budapest Convention: Directive 2000/31/EC on electronic commerce; Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography; Directive 2013/40/EU on attacks against information systems; Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union; Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

In general, as the systemic analysis of the provisions of the above directives attests, the security system against cybercrime and its counteraction is realized either through complex interaction of law enforcement agencies or through specially created agencies to combat cybercrime in the national law enforcement system. Instead, the security police are not mentioned at all in the above Directives, which gives every reason to claim that it can be used at least in the field of protection of servers, networks and computer databases.

The countries of Eastern Europe have a centralized system of law enforcement agencies which is identical to Ukrainian system, but even in these countries the government has significantly reduced the functions of the security police. For example, law enforcement agencies, whose functions are identical to the Ukrainian security police, are still operating in Poland and Hungary. Instead, in Romania, Slovenia and the Czech Republic, the state security guard agencies are minimized, and their main functions are the protection of high public officials [4].

A characteristic feature of the British police system is that all British police officers (including the state security guard service) are vested with relevant rights in pre-trial criminal investigations [14]. These functions are explicitly provided by The Policing and Crime Act 2017, and, in view of the subject matter of this study, suggest that the UK police are involved in the investigation of crimes committed, and the effectiveness of this involvement and prompt response of the security police significantly increase the effectiveness of counteraction to crime. Security police agencies in the UK do not have such a clear structure as in Ukraine, but there are special police units in the country, in particular: police of the National Atomic Energy Authority, police of the Ministry of Defence, the Civil Aviation Police, police of the Port of London Authority and other ports - they all ensure security of the respective facilities, law and order, which is their top priority.

In addition, since 2001, after the reform of law enforcement agencies, the so-called community protection officers (hereinafter – CPOS) were introduced into the UK police, replacing the patrol and duty service and being incorporated into the municipal police to provide official presence of authorities in residential areas to improve quality of life and public order. The CPOS are vested with additional powers to detain crime suspects and the ability to enforce certain safety and public order standards. But their main purpose is that they stay on the territory of municipal property facilities (residential houses, public utilities, etc.) and, in fact, provide their safety at a non-contractual basis, serving as police constables [9].

The experience of the security police in France is limited to the following specialized units within the National Gendarmerie: Civil Aviation Gendarmerie; Gendarmerie of the Defence and Industrial Complex; Gendarmerie at the Nuclear Facilities [13]. The process of finding opportunities to expand the functions of these bodies of the National Gendarmerie was launched from the very beginning of their functioning [13]. In essence, they performed purely protective functions for strategic objects of the state, but in 2016, these bodies became part of the counter-terrorism system, including cyberterrorism. The National Plan of Intervention and Counteraction to Terrorism was adopted, which provides the involvement of all three above-mentioned National Gendarmerie agencies in counter-terrorism activities at their respective objects. But the legislation of France excludes other powers in counteraction to cybercrime or more extended functional load on security police.

The German security police are called Wachpolizei, but it exists only in the federal states: Berlin, Giessen, Saxony, Bremen, as well in the city of Berlin, and their main task is the protection of objects (usually government agencies, foreign missions). Security police officers serve in the police uniform (with insignia of distinction), while being employed without police officer status. Wachpolizei are deprived of the ability to apply exigencies in the field of public order beyond the scope of guarding objects entrusted to these units. The legislation does not provide extension of the powers of these security police agencies to counteract to cybercrime, but their status – semi-official – opens up opportunities for expanding their functional load as private entities in the security services market.

Thus, according to the analysis of the Ukrainian legislation, the security police have a monopoly position in the security services market, since this police unit has a legitimate reason not only to use special means and weapons against offenders, but also legal coercion. Such preferences, as well as broad powers in the field of personal guarding and in guarding objects, create a high law enforcement and preventive potential of the police in the areas of combating crime and counteraction to crime, including cybercrime. Instead, the legislation of the vast majority of European countries does not give any preference to national law enforcement agencies like the Ukrainian security police. Most of their functions are limited solely to the protection of state and municipal bodies, institutions, organizations and industrial objects, as well as politicians. However, municipal police are limited, and in most countries even denied the opportunity to be used as additional law enforcement agencies in combating cybercrime.

4. Discussion

Analysing the above results of the study of the security police status and the degree of their involvement in the processes of combating cybercrime and counteraction to it, it is logical to conclude that, even where security police act as a separate structural unit of national police authorities, their functions are significantly limited only by guarding objects of national importance. Instead, the logical question is whether computer networks, servers, technology data centers and information archives storing electronic information can or should be considered as the objects of national importance? Obviously, they should, this is because most of the spheres of public relations today are computerized, so the vast majority of socio-economic processes are managed through computer networks that are subject to cybercrime.

The first step towards extending the boundaries of involvement of security police in combating cybercrime is the ratification of the Budapest Convention, which will allow developing unified approaches to the implementation of some operational and investigative measures in the international cooperation [15], including cyberspace. Ukraine has already accomplished this task, but in addition to ratification, it also requires the establishment of an appropriate mechanism for interaction, international cooperation and coordination of joint efforts.

According to [16], the main problem of unrealizing the potential of security police in the European countries in the context of cybercrime is the structural and cultural constraints of traditional police agencies that have led to a lack of security in the online world. This lack of security means that crimes committed online are hardly reported or ignored by law enforcement agencies; and the police often does not have sufficient resources to effectively counter cybercrime [16]. But in [17], the author notes that the fight against cybercrime is not a simple case of expanding the current crime-combating paradigm by increasing the number of police officers. The nature of the Internet requires addressing the problem of cybercrime by finding new resources and realizing existing capabilities both in the existing law enforcement agencies and by involving private actors, each capable of enhancing the intellectual capital of the law enforcement system in the context of cyber space security [17]. In [18], the need to transform not so much the institutional foundations of the functioning of police agencies but the extension of their organizational capacity was emphasized, in particular by joining efforts of different police authorities and delegating powers or deconcentrating them in those areas where combating crime is ineffective. Objectively, cybercrime is difficult to prevent, and it is therefore advisable to shift the focus to counteracting it, responding quickly, and overcoming the consequences of those crimes.

This can be achieved by extending the powers of the security police, which should first be empowered to secure computer networks and servers, as well as electronic databases stored in data centers. In addition, security police can carry on permanent patrolling in the most marginalized areas of cities, not replacing patrol police, but only enhancing the potential of law enforcement activities.

In this context, the researcher demonstrates the successful experience of Poland and Hungary in introducing municipal security police, which, despite its non-government but purely municipal status, are capable of accomplishing the task of guarding objects, while applying legal coercion [5]. The latter testifies to the ability of municipal security police to perform not only security functions but also preventive ones. It is the location of such police units in cities or in specific territories that reduces the manifestation of criminogenic factors [5]. Unfortunately, the municipal police do not have such authority in Ukraine, and its legal status of a municipal enterprise or municipal institution also excludes the possibility of using weapons. In [19], we find confirmation of the conclusions that municipal security police are more capable of performing some security functions than the national police. The researcher made this conclusion on the basis of an analysis of the municipal police system in Hungary and the Czech Republic, where the municipal security police have the right to withdraw the means of committing a crime or to check the potentially dangerous behaviour of persons for illegal signs [19]. In [3], the author points out that the security police are more of an atypical manifestation for most national law enforcement systems in the EU, but where they exist – expanding their functions is unlikely to be appropriate, as they serve as the militarized guards of the most important objects for public security.

In part, the study [11] also contains this conclusion. The reasonability of the transfer of some functions, in particular, the functions of guarding, to private security entities was noted [11]. According to the researcher, this will significantly reduce the cost of police maintenance, but will increase the efficiency and quality of security services, enabling private entities to use more modern equipment, including cyber-equipment and new-generation information systems [11]. Such opportunities can give a false idea of the ability to coordinate and co-operate with the public and private sectors in combating cybercrime.

However, the view of the transfer of protection functions from police to private entities is also supported in [20], where the authors advocate the privatization and deconcentration of the security services market as a first step towards the privatization of the state's police function. In our view, the only rational conclusion from the perspective of these researchers is that not so much privatization is needed, but rather the deconcentration of the police function through the transfer of most powers, in particular in the field of security police, from the national government to local self-governments. Expanding the powers and capabilities of the municipal security police will increase the potential for counteracting cybercrime, since such police can be created in the territories of municipalities with high levels of informatization, or where a large number of IT professionals reside, or where objects that could potentially be targeted by cyber-attacks are located.

This potential of the municipal security police is discussed, in particular, [21] demonstrates the real ability of the new police to ensure a high level of public safety on the example of the Netherlands. The point is that, according to scholars, the municipal security police should stop patrolling the streets and create a network of the so-called security posts, which will be located in the most dangerous and marginalized urban neighbourhoods [21]. According to [8], such a network will ensure the presence of authorities, and therefore provide the protection of objects that are of major municipal importance or are considered the riskiest segments of municipal security [8]. In our view, this approach shows not a tendency towards the emergence of new security police in those countries where it did not exist in the national police segment, but rather a tendency towards enhancing the preventive and law enforcement potential of police authorities.

In addition, assigning both security and prosecution functions (as in the UK) will significantly increase the mobility of the entire law enforcement system in its response to cybercrime.

The undeniable difficulty of engaging security police in combating or counteracting cybercrime is that this type of crime is committed in a virtual world with no physical assets to be protected. Instead, the entire virtual world exists thanks to physical devices and storage media, as well as computer networks, so it is logical to use the municipal security police and to ensure smooth operation of such objects, including preventing their physical break-in or penetration into their territory.

It was demonstrated on the example of Nottingham that engaging community protection officers (CPOS) in maintaining public order does reduce crime rate, including cybercrime, at least those varieties that are related to bank and payment instruments fraud, theft of personal data, distribution of pornographic products, antisocial, chauvinist and racist appeals, etc. [6]. On the other hand, the researcher points out in [22] that the extension of the police security function is not sufficient to effectively combat cybercrime. It is important to develop programs for the interaction of different police entities with each other, to create a single flexible and even project-based network of law enforcement agencies capable of engaging in combating and counteracting cybercrime within certain time in order to eliminate a specific danger. Such procedures are described in the Standard Operating Procedures, the document that has an interagency nature and should provide an algorithmization of the process of ensuring a particular state of public security with the involvement of certain law enforcement agencies [22]. However, this plan which was developed by the special office of the UN Police Mission, has no specific focus in the context of cybercrime. It is only a means of accumulating the potentials and efforts of law enforcement agencies of different status, but it can in no way be considered as an algorithmization of their action, and in particular of the security police, in the process of counteracting cybercrime. Unlike national police, the CPOS do not have a clear link to secured objects (nuclear facilities, military facilities, etc.). The main criterion for choosing of the so-called security posts by those agencies is to solve the problems of combating crime in a specific territory. Therefore, by placing the CPOS in the appropriate local area, the municipal authority seeks to maximize the concentration of law enforcement agencies on it, which, in turn, has the relevant response of the criminal world. Thus, we support the positions outlined above that the existence of a municipal security police will significantly increase the effectiveness of the preventive function of those law enforcement agencies. However, prevention is embodied not in the subjectivity or objectivity of the impact, that is, not by directing the efforts of security police to particular subjects or objects of crime, but by creating such security conditions when the crime itself becomes a problematic and complicated process.

In this context, the importance of extending the functioning of the municipal security police as a means of increasing the overall level of decriminalization of society and reducing opportunities for victimization behaviour is noted. Due to the constant presence on municipal objects, which far outnumber state objects, it creates a stable idea of the high level of concentration of law enforcement agencies in a particular locality. Wachpolizei – municipal security police in Germany – is capable of performing far more functions than just guarding municipal objects, and their purpose can be substantially expanded by giving new functions by municipal acts only. We fully share the last thesis. By the way, the value of municipal security police protection in combating cybercrime would be ensured through the ability of municipal authorities to manage the activities of the police more flexibly, since it is funded from local budgets.

We believe that the real potential of municipal security police to combat cybercrime is revealed through certain elements of their functioning that are not relevant to most other law enforcement agencies that focus on such crimes. Moreover, it is the municipal nature of the functioning of those security police authorities that can compensate for the lack of flexibility of the nationwide police system, as well as the mobility to respond to cybercrime.

But, for example, researchers in [7] argue that the highest efficiency of the cybercrime counteraction subsystem is ensured by the high concentration of interagency links and inter-institutional interaction between different entities of national law enforcement agencies [7]. In our view, municipal security police are so mobile that they can be integrated into any system of interagency interaction between government institutions for combating cybercrime.

In general, the process of adaptation of municipal security police to the system of counteracting and combating cybercrime can be represented as follows (Figure 2).

Thus, since the municipal police of Ukraine is not directly subordinated to and is not maintained at the expense of national police authorities, but only acts on the organizational and legal basis determined by the state, it is advisable to present its separate impact on the cybercrime counteraction system in the EU (Figure 3).

Therefore, we see that municipal security police is a means of enhancing law enforcement and preventive potential of the police in the country, which will increase the effectiveness of combating cybercrime. For Ukraine, this experience is extremely useful and necessary, as modern security police, while performing its functions, only monopolize the security services market but does not solve any crime prevention tasks. The police in Ukraine should have the same functions as the constables in the UK, that is, have powers in the field of criminal proceedings and prosecution. Due to the high mobility, flexibility and responsiveness, municipal security police can become an effective means of counteracting cybercrime. And by creating a network of security (observation) posts at municipal objects, security police will increase the concentration of law enforcement agencies in a particular area. The latter will reduce crime rates.

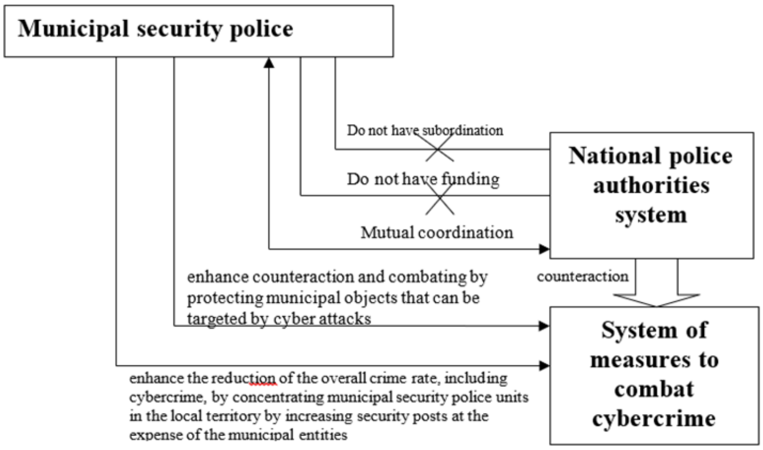
Municipal security police
Do not have subordination
Do not have funding
Mutual coordination
National police authorities system
counteraction
enhance counteraction and combating by protecting municipal objects that can be targeted by cyber attacks
System of measures to combat cybercrime
enhance the reduction of the overall crime rate, including cybercrime, by concentrating municipal security police units in the local territory by increasing security posts at the expense of the municipal entities

Figure 2. Influence of municipal security police on the system of combating cybercrime and their relationship with the system of national police authorities

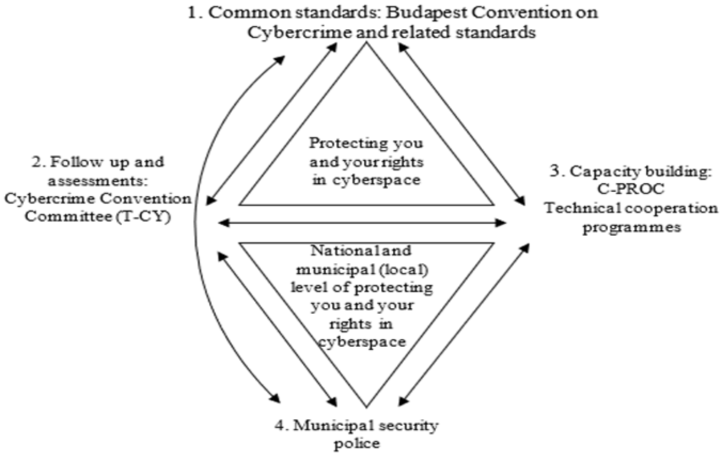
1. Common standards: Budapest Convention on Cybercrime and related standards
2. Follow up and assessments: Cybercrime Convention Committee (T-CY)
3. Capacity building: C-PROC Technical cooperation programmes
4. Municipal security police
Protecting you and your rights in cyberspace
National and municipal (local) level of protecting you and your rights in cyberspace

Figure 3. Mechanism for counteraction to cybercrime in the EU, taking into account functioning of municipal security police

5. Conclusion

To summarize, the following main conclusions can be drawn. First, the national police systems of most EU Member States include special units that perform the functions of protecting the most important objects for public safety purposes (mainly industrial, power, nuclear objects, etc.). At the same time, these countries do not have security police authorities that would perform the same functions as the police in Ukraine.

Second, the main functionality of the police is aimed at ensuring the physical security of objects. Instead, cybercrime has a virtualized manifestation, although it is important to conclude that cybercriminals may also target computer networks, data centers, servers and other computer hardware (physical form). This means that the security police will ensure performance of a preventive function in the field of combating cybercrime.

Third, we have found the possibility of extending law enforcement potential of the security police in the analysed area through the creation of a network of municipal security police which will, in addition to the security functions, also have criminal prosecution functions (similar to the CPOS in the UK). In Ukraine, municipal security police are seen as an extremely effective tool to enhance the capacity to perform a preventive and criminal prosecution function in the field of combating cybercrime. It carries out its activities by forming a network of security posts located in the most marginalized parts of communities, as well as at municipal and state objects. The fact that municipal objects outnumber state objects creates an excessive concentration of law enforcement agencies in a rather small territory. Thus, there is an indirect but extremely effective impact on reducing the level of criminogenic situation and reducing the number of crimes, including cybercrime.

References

[1]. Bilenchuk, P., & Borysova, L. (2017). Legal Protection of the Computer Programs. *History & Law Journal*, *1*(9), 82-87.

[2]. Yakimova, E. M., & Narutto, S. V. (2016). International cooperation in cybercrime counteraction. *Russian Journal of Criminology*, *10*(2), 369-378.

[3]. Bilas, A. I. (2016). *Law enforcement in EU countries: a comparative legal study*. PhD thesis. National Academy of Internal Affairs.

[4]. Kryshtanovich, M. F. (2015). European experience of state administration of police and possibility of his use organs is in Ukraine. *Actual problems of public administration*, *1*(47), 287-293.

[5]. Orlov, V. A. (2018). Municipal police in the EU post-socialist countries: comparative analysis. *Law journal of Donbass*, *2*(63), 5-16.

[6]. Butler, M. (2015). *Standard Operating Procedures: Community Protection Officers*. Nottingham City Council.

[7]. Sindhu, K. K., Kombade, R., Gadge, R., & Meshram, B. B. (2014). Forensic investigation processes for cyber crime and cyber space. In *Proceedings of International Conference on Internet Computing and Information Communications* (pp. 193-206). Springer, New Delhi.

[8]. Probert, A. (2014). A revolutionary way of working with police force. *Insight, 9*, 18-32.

[9]. Cashmore, J. (2017). Have community protection officers (CPOS) met expectations? *Internet Journal of Criminology.*

[10]. Loveday, B., & Smith, R. (2015). A critical evaluation of current and future roles of police community support officers and neighbourhood wardens within the Metropolitan Police Service and London boroughs: Utilising 'low-cost high-value'support services in a period of financial austerity. *International journal of police science & management*, *17*(2), 74-80.

[11]. White, A. (2014). Post-crisis policing and public–private partnerships: The case of Lincolnshire Police and G4S. *British journal of criminology*, *54*(6), 1002-1022.

[12]. Khimchenko, I. A. (2014). *The Information Society: Legal Issues in the Context of Globalization*. PhD thesis. Institute of State and Law of the Russian Academy of Sciences.

[13]. Smith, M. R., & Sakhno, A. (2018). *Face-to-face with a new reality: exacerbation of security and security issues against a backdrop of scarce resources A review of the security and security market in Ukraine. Special Report of the Commercial Service of the US Embassy in Ukraine*. US Embassy in Kiev.

[14]. Sobol, E. J., & Kolomojtsev, S. S. (2010). Experience of the Organization and Activity of Police of the Leading Countries of Europe. *Law Forum*, *2*, 461-466.

[15]. Borovyk, P. L. (2011). Analysis of the provisions of the Council of Europe Convention on the fight against cybercrime in order to combat child pornography on the Internet. *Bulletin of the Academy of the Ministry of Internal Affairs of the Republic of Belarus*, *4*, 273-283.

[16]. Huey, L., Nhan, J., & Broll, R. (2013). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice*, *13*(1), 81-97.

[17]. Loveday, B. (2015). Police management and workforce reform in a period of austerity. in P. Wankhade & D. Weir (eds.), *Police Services Leadership and Management Perspectives* (pp. 115-127). Springer.

[18]. Crawford, A. (2013). The police, policing and the future of the 'extended policing family'. *The future of policing*, 173-190.

[19]. Gudz, T. (2015). Territorial, material and financial grounds of police activity organization in foreign countries. *Public Law*, *4*, 84-92.

[20]. Travis, A., & Williams, Z. (2012). Revealed: Government plans for police privatisation. *The Guardian*, *2*, 2012.

[21]. Terpstra, J., van Stokkom, B., & Spreeuwers, R. (2013). *Who Patrols the Streets?: An International Comparative Study of Plural Policing*. The Hague: Eleven International Publishing.

[22]. Akyar, I. (2012). Standard operating procedures (what are they good for?). *Latest research into quality control*, 367-391.