NATIONAL AUDIT OFFICE OF LITHUANIA
• BRINGING BENEFITS •

IS CYBERCRIME COMBATED EFFECTIVELY

16 July 2020

No VAE-7

SUMMARY

The Importance of the Audit

Despite the fact that the development of information technology has led to many positive changes, it has also influenced the emergence of criminal offences in the cyberspace. In accordance with the Convention on Cybercrime[1], these offences include offences against the confidentiality, integrity and availability of computer data and systems, and other offences in cyberspace: Internet fraud, offences related to the sexual exploitation of children, violations of copyright and related rights, acts of a racist and xenophobic nature. In the conclusions of the EU Council of 2015 on the renewed EU Internal Security Strategy[2] for the period 2015–2020 it is declared that the fight against cybercrime is one of three key security priorities. Based on the European Cybersecurity Strategy[3], the National report on Serious and Organised Crime Threat Assessment 2019[4] by the Europol's European Cybercrime Centre (EC3) and the World Economic Forum's Global Risks Report 2020,[5] it is predicted that the scope and potential harm of cybercrimes will only increase in the future, and rapid changes in information and communication technologies (e.g. cloud computing) can lead to new challenges as well. Criminal offences in this area are to be observed as a growing serious threat to public security. A study[6] conducted in 2018 by the US computer security software company "McAfee" together with the Centre for Strategic and International Studies shows that global business expenditure due to cybercrime amounted to almost EUR 700 billion[7], which accounted for 0.8 per cent of global GDP.

[1] The Convention on Cybercrime, adopted in Budapest on 23/11/2001, was ratified by Law No IX-1974 of the Republic of Lithuania of 22/01/2004 and by Law No X-674 of 08/06/2006 – Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

[2] Internet access: https://vrm.lrv.lt/uploads/vrm/documents/files/LT_versija/Viesasis_saugumas/. Strategijos/2015_Tarybos_isvados_del_VSS.pdf.

[3] Internet access: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex:52017JC0450.

[4] Internet access: https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf .

[5] Ibid.

[6] " Economic Impact of Cybercrime". Internet access: https://www.mcafee.com/enterprise/en-us/forms/gated-form-thanks.html?docID=5fee1c652573999d75e4388122bf72f5&tag=ec&eid=18TL_ECGLQ1_CT_WW.

[7] The estimated cost of almost USD 600 billion was recalculated in Euro.

According to the survey [8] of the US software company "WebsiteBuilderExpert" on cybercrime risk in EU countries in 2018, Lithuania ranks 6th among 28 EU countries as one of the countries with the highest risk of cybercrime. According to a Eurobarometer survey carried out in 2019, 73 per cent of the Lithuanian population believe that the risk of becoming a victim of cybercrime is increasing, and 42 per cent of the residents are not well informed about the threats of crime in the cyberspace.

In order to assess the effectiveness of cybercrime prevention and investigation, it has been decided to carry out an audit of the cybercrime prevention and investigation system.

Objective and Scope of the Audit

The objective of the audit is to assess whether the investigation and prevention of cybercrime ensure a safe environment for the public in the cyberspace.

Key audit questions:

- whether preventive activities are planned and implemented in such a way as to ensure the achievement of the objectives of cybercrime prevention activities;
- whether the investigation of cybercrime is ensured;
- whether conditions have been created for the improvement of investigation in the field of cybercrime.

Audited entities:

- The Prosecutor General's Office which directs the territorial prosecutor's offices and supervises their activities, develops a common practice for the pre-trial investigation of criminal acts and the supervision of actions in criminal proceedings, organises professional and in-service training of prosecutors[9].
- The Police Department under the Ministry of the Interior, which organises, coordinates and supervises the implementation of the Police tasks, as well as organises and implements the management of subordinate police bodies[10].
- The Ministry of National Defense, which formulates the cybersecurity policy and organises, controls and coordinates its implementation[11].
- The Ministry of Justice, which formulates the policy in the areas of criminal law, criminal procedure, execution of sentences and organises, coordinates and controls the implementation of these State policies[12].

The audited period is 2015–2019. In order to assess changes and compare data, in some cases both the earlier and 2020 data were used to collect the audit evidence.

[8] Internet access: https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/.

[9] The Law of the Prosecutor's Office, Article 8.

[10] The Regulations of the Police Department under the Ministry of the Interior of the Republic of Lithuania approved by Government Resolution No 98 of 29/01/2001, p. 10.

[11] Law on Cyber Security, Article 4.

[12] Regulations of the Ministry of Justice of the Republic of Lithuania approved by Government Resolution No 851 of 09/07/1998, p. 7.

In the course of the audit, the lawfulness and validity of procedural decisions of the pre-trial investigation were not assessed as according to the Law of the Prosecutor's Office, the prosecutor's procedural activities are controlled by a senior prosecutor and a court[13]. A system for investigating cybercrime, which should allow these decisions to be made comprehensively and quickly, was assessed. While performing the analysis of pre-trial investigations, statistical data of pre-trial investigations completed in 2015 was not analysed, because according to the data of the Lithuanian Criminal Police Bureau, when the Integrated Information System of Criminal Process was launched in 2015, part of the data may be inaccurate.

The audit has been performed in accordance with the Public Auditing Requirements and the International Standards of Supreme Audit Institutions. Audit scope and the applied methods are described in more detail in Annex 2 "Audit scope and methods " (p. 71).

Key Audit Results

As more and more activities are being transferred to the digital space by the society, more criminal offences are also being moved there. With the growing amount of cybercrimes, the society must be prepared to recognise the threats of cybercrime and be able to protect itself from them. Forces capable of preventing and investigating this type of crime must be formed, but shortcomings have been identified in cybercrime prevention and investigation processes and secure cyberspace is still not ensured for the society.

1. Preventive activities do not create the conditions for the society to feel secure in cyberspace

Preventive activities for cybercrime are carried out by the Police and other institutions: the National Cyber Security Centre under the Ministry of National Defence, the Communications Regulatory Authority, the State Data Protection Inspectorate, the State Consumer Rights Protection Authority, the Office of the Inspector of Journalist Ethics, the Ministry of Culture, the Information Society Development Committee, the Government Office. During the period 2015–2019, the Police bodies alone implemented approximately 1.5 thousand various preventive measures, mainly focused on educational activities during events and providing information on the Internet. However, the participating institutions operate within their area of competence and according to their priorities, do not coordinate preventive measures with each other, do not carry out an impact assessment of preventive activities in cybercrime, and an inter-institutional system for planning, coordinating and measuring the impact of preventive activities at the national level is not established. For these reasons, similar preventive measures are being implemented (e.g., educational activities on the subject of Internet fraud were carried out by 5 institutions) which do not produce the necessary result. According to the Eurobarometer survey, in 2019, compared to 2018, Lithuania shows a 16 per cent increase (from 28 per cent to 44 per cent, respectively) in residents who believe that they are not able to protect themselves from cybercrime.

[13] The Law of the Prosecutor's Office, Article 4(2).

Blocking rights, which should restrict access to unwanted and harmful content on the Internet, have been granted to 7 institutions. We found that by February 2020 a total of 511 websites were blocked at the national level. As a result of the blocking actions, another mirror site is created[14], for instance, out of 397 sites blocked by Gaming Control Authority, 297 were mirror sites. Those who distribute unwanted and harmful content on the Internet are able to circumvent the blocking mechanism, therefore, these measures are of a temporary nature, while illegal and harmful content remains not removed. As a result, the residents remain at risk of being victimised by potential crimes, and repeated blocking actions increase the administrative burden for authorities and businesses implementing binding instructions. When implementing the blocking powers, the institutions apply different legislation which sets out different enforcement regimes for blocking rights: different procedural steps, periods, choice of methods of blocking.

2. Weaknesses in cyber incident management do not allow to identify all incidents that may be criminal offences

The Police do not manage all information about cyber incidents that may be criminal offences, as not all cybersecurity entities (19 out of 143 surveyed by auditors) report cyber incidents that are potentially criminal offences in cyberspace to the Police. The State Data Protection Inspectorate never provided such information to the Police in 2015–2019 and the National Cyber Security Centre instructs cybersecurity entities to address the Police individually. The Police and the National Cyber Security Centre do not exchange the available data about online events and incidents. This situation is caused by weaknesses in the management of cyber incidents. There are no criteria (a general taxonomy[15]) to identify which cyber incidents are potentially cybercrimes. There is also no clear regulation on what cybersecurity entities are required to inform – the Police or the National Cyber Security Centre about cyber incidents possibly having elements of a criminal offence. A lack of methodological leadership, advice and training to enhance cybersecurity entities' ability to identify and respond to criminal offences: 64 per cent of surveyed cybersecurity entities do not know how to assess the loss or damage of a crime, 51 per cent – how to collect and save electronic evidence properly and 27 per cent – how to respond to a possible cybercrime. In addition, it has not been possible to manage cyber incidents, which are potential cybercrime, on a one-stop-shop principle basis.

The Lithuanian Criminal Police Bureau does not actively monitor and analyse cyber incidents, which are potentially criminal offences and does not allocate sufficient human resources to these activities (one official works with cyber incidents and during the period 2015–2019 he conducted 9 cyber incident investigations). Without managing all the information about cyber incidents that may be cybercrimes, the Police may not respond in time to the criminal offences committed in cyberspace and fail to assess the extent of these threats.

3. No conditions have been created to conduct cybercrime investigations effectively

[14] Mirror sites are websites where the Internet domain name is almost identical to the original website and several letters, numbers, other characters, changes in the ending of the domain, or the like are added or removed.

[15] Descriptions of certain features (references to legislation) that allow different types of cyber incidents to be linked to certain criminal offences.

In 2015, specialised units of the Criminal Police for crimes in cyberspace began operating in the Chief Police Commissariats, which were assigned to prevent, detect and investigate criminal offences in their territory against the security of electronic data and information systems, and the criminal offences committed in cyberspace. The performance of these units is not sufficient. It was found that in 2019, compared with 2016, there was a 9 per cent decrease in the number of pre-trial investigations transferred to court and it is below the target[16] of 40 per cent (38 per cent in 2016, 39 per cent in 2017, 37 per cent in 2018 and 29 per cent in 2019). 40 per cent of cybercrime pre-trial investigations last longer than the target deadline of 9 months[17]. In addition, 11 per cent (21 out of 191) of pre-trial procedural decisions examined in this area that were suspended, terminated or pre-trial investigations were refused to initiate, were annulled by prosecutors during the period 2017–2019. The effectiveness of these investigations is influenced by the insufficiently effective management model of specialised units and the organisation of training of officials and prosecutors.

Insufficiently effective management model of cybercrime specialised units

Weaknesses identified by the audit in the management of specialised units:

- At the national level, there is insufficient identification of systemic cybercrime. Although data analysis is carried out at the level of the County Chief Police Commissariats in order to detect systemic crimes, the Prosecutor General's Office detects pre-trial investigations carried out in different commissariats, which are not identified as part of systemic crime and are not combined. For instance, from 19/08/2019 to 18/02/2020, 68 pre-trial investigations were launched in different pre-trial institutions which were not combined into a systemic one. The Lithuanian Criminal Police Bureau does not have all information about identified systemic crimes. From June 2018 to March 2020 the Lithuanian Criminal Police Bureau received 11 service reports about systemic cybercrimes from the Vilnius County Chief Police Commissariat, while other units did not provide such information. Failure to identify all systemic crimes leads to the loss of the opportunity to assess the real extent of the damage caused by criminal offences, the number of victims and perpetrators.
- There is a lack of specialised capacity to investigate cybercrimes. In the four specialised units conducting the most pre-trial cybercrime investigations, the acceptable workload (up to a maximum of 6 pre-trial investigations at a time) of officials is exceeded. Workloads of some officials exceed the established norm up to 3 times (i.e., in Vilnius specialised unit some officials conducted 16–20 pre-trial investigations at a time, in Kaunas - 14). These workloads arise because the specialised units are incomplete: in 2019, the percentage of posts not occupied in cybercrime was 22 per cent on average. In addition, the workload is also increased by non-preventable cybercrimes committed from places of detention. For instance, in 2019, electronic fraud from imprisonment institutions investigated by specialised units in Vilnius, Kaunas and Klaipėda accounted to 8–16 per cent of all crimes of this nature registered that year. In

[16] A description of the procedure for applying internal control measures of the main activities of the Police carried out by the Lithuanian Criminal Police Office Order approved by the Order No 38-V-80-(1.10-38E) of the Head of the Lithuanian Criminal Police Bureau of 14/07/2017, Annex 2.

[17] Ibid.

order to redistribute and reduce workloads per an official, pre-trial investigations are assigned to the officials performing the intelligence function, thus reducing the scope of intelligence actions in this field. Insufficient human resources do not make it possible to conduct pre-trial investigations qualitatively and within the shortest time limits.

- The specialisation of Police units and prosecutors in cybercrime has not been sufficiently detailed. The current specialisation procedure and established practice do not ensure that cybercrime, which must be investigated in specialised units, is directed only to specialised officials and is managed only by specialised prosecutors. In 2016-2019, non-specialised officials performed 62 per cent of all cybercrime pre-trial investigations on average, of which 11 per cent on average were attributed to Chapter XXX of the Criminal Code, which is the competence of specialised units. 28 per cent of non-specialised prosecutors were in charge of pre-trial investigations of specialised units. Due to insufficiently detailed specialisation, some of the complex investigations can be carried out and managed by officials and prosecutors with insufficient expertise.
- Long queues of investigation of information technology objects, for instance, in the Criminal Investigation Department of Vilnius County Chief Police Commissariat, the waiting time for the investigation of objects is about 19 months, and in the Lithuanian Police Forensic Science Centre – about 10 months. As a result, these queues take time to investigate cybercrime, which can result in the loss of digital data relevant to the investigation.

These shortcomings of management do not allow cybercrime to be revealed quickly and comprehensively and do not fully employ all possibilities to investigate these criminal acts in the interests of the State and society.

Insufficiently organised training for specialised officials and prosecutors

There is no cybercrime training programme for specialised officials and training is carried out only according to their needs, which do not cover the courses recommended in IOCTA reports. We found that between 2015 and 2019, 30 per cent of specialised officers were attended any training. Individual joint training for prosecutors and officials is also organised. 70 per cent of specialised prosecutors and officials interviewed by auditors indicated that training in this area was insufficient.

The network of specialised prosecutors for cybercrime is still not fully operational and there is no network of officials to exchange best practices and experience among the participants of the system. In addition, 68 per cent of prosecutors interviewed by auditors and 62 per cent of officials indicated that there is a lack of new methodological documents that could facilitate the practical investigation of cybercrime, in particular, the collection and preservation of electronic evidence and the investigation of specific cybercrime. The lack of effective training does not allow for the development of competence of specialised officers and prosecutors and achieve better performance.

4. Insufficient attention to improve the prevention and investigation of cybercrime

The measures provided for in the Public Security Development Programme for 2015–2025 and the National Cyber Security Strategy to combat cybercrime are insufficient as they do not address the problems related to preventive activities; the removal of illegal and harmful content on the Internet; management of cyber incidents that are potentially cybercrime; identification of system cybercrime; development of specialised competencies; long queues of information technology objects investigation; insufficient profiling of cybercrime. Due to insufficient attention to the prevention and improvement of investigation of cybercrime, the results of investigation of this type of crime and public security in cyberspace may be further decreasing in the future.

Cybercrime profile covers crimes against the security of electronic data and information systems (Chapter XXX of the Criminal Code) and crimes related to child sexual exploitation online, however, it does not cover other criminal offences committed in cyberspace referred to in the Convention on Cybercrime: Internet fraud, crimes related to copyright and related rights violations, the crimes of a racist and xenophobic nature. Police registers do not collect, systematise and analyse all information about crimes in this field, and therefore do not analyse the actual scope and trends of cybercrime threats. The lack of complete information on these crimes can have a negative impact on strategic decisions and the appropriate response to changes in this area.

Various strategic planning documents set different target values for the indicator of the security of electronic data and information systems of investigated criminal offences (Chapter XXX of the Criminal Code). Since 2020, the Prosecutor General's Office and the Police Department have been seeking to investigate 50 per cent of such criminal offences, while the Inter-institutional Action Plan for the Implementation of the Public Security Development Programme for 2015–2025 sets a target investigation of 96 per cent.

Recommendations

To the Ministry of the Interior

1. In order to ensure that the implementation of cybercrime prevention activities have a greater impact on the ability of the country residents to recognise these threats, to establish inter-institutional planning, coordination and impact measurement of prevention activities in the field of cybercrime (1 key audit result).

2. To ensure more effective prevention of cybercrime at the national level by reducing the possibilities of people becoming victims of these crimes:

    2.1. To introduce measures to address illegal and harmful content on the internet (1 key audit result);

    2.2. To establish a common procedure for implementing blocking powers (1 key audit result).

To the Ministry of National Defence, Prosecutor General's Office and Police Department

3. To improve the identification of cyber incidents, that are potentially cybercrimes, of cybersecurity entities and to strengthen cooperation between the Police and the National Cybersecurity Centre in this area:

    3.1. To agree on the taxonomy of cybersecurity incidents and criminal offences in the cyberspace that would enable identification of which cyber incidents are potentially criminal offences (2 key audit result).

    3.2. According to the agreed taxonomy of cyber incidents and criminal offences in the cyberspace, to improve the existing mechanism of cyber incident management which would ensure that cybersecurity entities submit all cyber incidents that are potentially cybercrimes for further investigation at a one-stop-shop principle (2 key audit result).

4. In order to strengthen the capacity of cybersecurity entities that manage and control State information resources, to identify and respond appropriately to cyber incidents that may be cybercrimes:

    4.1. To organise training for cybersecurity entities that manage and control State information resources, ensuring that they are provided with the necessary legal and technical knowledge about cybercrimes (2 key audit result).

    4.2. To develop methodological documents on the assessment of incident damage/loss, collection and saving of electronic evidence (2 key audit result).

To the Police Department

5. In order to increase the effectiveness of cybercrime investigations:

    5.1. To review and improve the operational model of cybercrime specialised units in order to identify all systemic crimes at the national level, concentrate sufficient specialised investigative and expert capabilities and increase the scope of criminal intelligence activities (2 and 3 key audit results).

    5.2. To develop and approve a cybercrime training programme for specialised officials meeting the educational needs of officials in this field, with a particular focus on the development of new special competences and implement it (3 key audit result).

    5.3. To create a network of officials specialising in cybercrime and ensure that it is active (3 key audit result).

6. In order to manage information on all cybercrimes, to include in the scope of their profile all criminal offences committed in cyberspace and to ensure the collection, systematisation and use of this information for threat analysis and strategic decision making (4 key audit result).

To the Prosecutor General's Office

7. In order to improve the investigation of cybercrimes:

   7.1. To improve the specialisation regime of prosecutors so that all pre-trial investigations of cybercrime specialised officials are supervised by specialised prosecutors in this area (3 key audit result).

   7.2. To increase the extent of cybercrime training for specialised prosecutors and ensure that all specialised prosecutors participate in the training (3 key audit result).

   7.3. To develop and implement a joint training programme for specialised officers and prosecutors in cybercrime (3 key audit result).

   7.4. To assess the need for and develop methodological recommendations for the investigation of cybercrimes (3 key audit result).

To the Prison Department

8. In order to stop cybercrimes from places of detention, to develop and implement measures to prevent these crimes (3 key audit result).

To the Ministries of the Interior and National Defence

9. In order to improve the prevention and investigation of cybercrimes:

   9.1. To provide measures in national strategic planning documents to address current cybercrime issues (4-key audit result);

   9.2. To improve the criteria for the assessment of cybercrimes by aligning them in all strategic planning documents and by providing conditions for measuring the state of investigation of all these crimes (4 key audit result).

Measures and deadlines for the implementation of recommendations are provided in the report section "The Plan for the Implementation of Recommendations".