

EUROPEAN MOVEMENT ALBANIA

CYBERCRIME AS A GENERAL EUROPEAN THREAT

Róbert Bohunický



Funded by
the European Union



PUBLISHER

European Movement Albania (EMA)
Rr. Milto Tutulani, Nd.1, Ap. 3
Tirana 1019, Albania
Tel: +355 44 104 247
E-mail: info@em-al.org
Web: www.em-al.org

AUTHORS:

YEAR OF PUBLICATION:

July 2026

This publication was funded by the European Union. Its contents are the sole responsibility of European Movement Albania and its authors and do not necessarily reflect the views of the European Union.

The action "Building Partnership on Fundamentals: Empowering CSOs for the EU accession process", is being implemented by the European Movement in Albania, with the financial support of the European Union - IPA Civil Society Facility 2021, and in cooperation with the Academy of European Integration and Negotiations (AIEN), Slovak Foreign Policy Association (SFPA) and the Center for Transparency and Freedom of Information (CTFI).



Funded by
the European Union



1. Cybercrime as a General European Threat (EU Legal Basis)	03
2. Risks and Threats in the Digital Space	05
2.1. Fraud Involving Cyberspace	05
2.2. Child Abuse and Child Pornography on the Internet	06
2.3. Online Radicalization and Terrorism-Related Content	07
2.4. Broader risks associated with digital platforms and the use of social media (threats, defamation, personal attacks/threats to personal status, etc.)	08
3. Building Sufficient or Adequate Capacities to Combat Cybercrime	14

1. Cybercrime as a General European Threat (EU Legal Basis)

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime, is a fundamental international treaty aimed at combating cybercrime. It was adopted in 2001 in Budapest under the auspices of the Council of Europe and entered into force on July 1, 2004.

The main objectives of the Convention are to harmonize states' criminal laws in the area of cybercrime, to establish effective procedural tools for investigating cybercrimes, and to promote rapid international cooperation among states. The Convention primarily covers the following criminal offenses: unauthorized access to computer systems (hacking), unauthorized interception of data, damaging, deleting, or altering data, disrupting the functioning of computer systems, misuse of equipment or software to commit cybercrime, computer fraud, computer forgery, offenses related to materials depicting child sexual abuse, and copyright infringement through information technology. Procedural provisions (the Convention also regulates the powers of law enforcement authorities): the seizure and preservation of electronic evidence; the search and seizure of data stored on computers; the collection of traffic data; and the interception of data communications (subject to the conditions of national law).

With regard to international cooperation, the document primarily regulates mutual legal assistance, the extradition of offenders, and the establishment of a network of contact points available 24 hours a day, 7 days a week, to handle urgent cases.

Albania is a signatory to this Convention. (Currently, all relevant legislation should be duly aligned with the Convention.) In 2022, the Second Additional Protocol to the Budapest Convention was also adopted, which improves the ability to obtain electronic evidence from service providers and strengthens cross-border cooperation in the investigation of cybercrime. Its main objective is to improve the collection of electronic evidence in the investigation of cybercrime and other crimes committed through information technology.

The original Budapest Convention of 2001 was drafted at a time when cloud services, social media, and global data centers were not yet so widespread. As a result, investigators often encountered various problems, such as data being stored in another country, the process of obtaining it through traditional international legal assistance taking too long, and the data potentially being deleted in the meantime. The Second Protocol is intended to significantly speed up this process.

The protocol's primary benefit: direct data retrieval from service providers (authorities can request data directly from internet service providers, cloud service operators, social media platforms, and hosting companies).

This primarily includes user identification and authentication data, contact information, and user account information. The amendment introduces mechanisms that enable faster transmission of requests between countries, the use of electronic communication channels, and better coordination of investigations. Countries can more easily form joint investigation teams to investigate international cases of cybercrime.

The protocol also regulates the protection of personal data and data handling procedures, and ensures the integrity and admissibility of data in legal proceedings. The protocol is intended to be more effective primarily for investigating cyberattacks, large-scale online fraud, ransomware, identity theft, and the dissemination of illegal content. This is a major international instrument that responds to the reality of cloud services and the global internet. It makes it possible to obtain electronic evidence significantly faster than was possible under the original 2001 convention.

The Budapest Convention is today considered the most significant international legal instrument in the fight against computer and cybercrime, and has been acceded to not only by European states but also by many countries from other parts of the world, including the United States, Japan, Australia, and Canada.

Supplementing the protocol are additional EU Commission regulations that specify the format of the data to be transmitted, its admissibility in criminal proceedings, and other details regarding the investigation of computer crime offenses.

Key entities in international police cooperation include Europol (EC3), Interpol, and Eurojust, with Europol's EC3 in particular holding a particularly significant position and role. EC3—the European Cybercrime Center—is a specialized unit operating within Europol that coordinates the fight against cybercrime in the member states of the European Union. Its main objective is to support law enforcement agencies in preventing, detecting, and investigating serious and organized cybercrime. EC3 provides EU member states with: operational support in investigating cross-border cybercrimes, coordination of international police operations, analysis of operational information on cyber threats, digital forensic and technical support, strategic analyses and assessments of cybercrime trends,

specialized training and capacity building for law enforcement agencies, and support for international cooperation with both the public and private sectors. In the area of online child sexual abuse, this support takes the form of analysis of child sexual abuse material (CSAM), online grooming, analysis of live streams of child sexual abuse, and the identification of victims and perpetrators. EC3 works closely with institutions and agencies that play a significant role in combating cybercrime. These include, for example, the European Union Agency for Cybersecurity (ENISA), national police forces, national cybercrime units, CSIRT/CERT teams, technology companies, financial institutions, and academic institutions.

Practical recommendation:

Intensify cooperation between the cybercrime unit and Europol's National Focal Point, including the mutual sharing of experiences (information on current trends and the situation regarding modus operandi in the country as well as in other EU countries, observed changes in forms of criminal activity in the field of cybercrime), and joint or mutual training activities. Also, intensify cooperation with EC3, which has extensive analytical data and can provide useful advice on preventive measures (for the police, government, and banking sectors).

2. Risks and Threats in the Digital Space

2.1. Fraud Involving Cyberspace

Main Types of Cybercrime Fraud

1. Phishing – fraudulent emails, text messages, or websites that impersonate trusted institutions (e.g., banks) with the aim of extracting users' identification and authentication data, passwords to applications or platforms, or payment card and payment method information

2. Spear phishing – targeted phishing aimed at a specific individual, group of individuals, or organization, in which the attacker uses information about the victim to increase the message's credibility (this may involve users of a specific web service or application)

3. Smishing – phishing carried out via SMS messages

4. Vishing – phishing carried out via direct telephone communication, in which the attacker impersonates, for example, a bank employee, police officer, or technical support representative (or another trusted entity)

5. Pharming – redirecting a user to a fake website in order to obtain their identification or authentication information, or payment details (username and password for a payment)

6. Online auction and classifieds scams – selling nonexistent goods or soliciting payment without delivering the ordered product

7. Online banking fraud – unauthorized transfers of funds using illegally obtained identification and authentication data, or malicious code installed on the victim's computer

8. Payment card fraud – misuse of payment card data during online purchases

9. Identity theft – the unauthorized acquisition and misuse of personal data to enter into contracts, take out loans, or create fake accounts.

10. Business Email Compromise (BEC)—a scam in which an attacker impersonates company management or a business partner and requests a transfer of funds to a fraudulent account.

11. Ransomware – malicious code that encrypts a user's data, after which the attacker demands payment to restore it

12. Romance scams – establishing a fake relationship online with the aim of gradually extorting money from the victim.

13. Investment and cryptocurrency scams – fake investment platforms or offers promising high returns, designed to obtain funds from victims.

14. Tech Support Scams – an attacker pretends to be a tech support representative and convinces the victim to install remote access software

These scams are among the most common forms of cybercrime, and their numbers are growing every year as a result of the development and widespread use of digital technologies and online services. The prevalence of individual forms typically varies by country and depends on the “popularity” of certain applications or platforms.

Practical recommendation:

In cooperation with Europol, monitor trends and the state of crime (in terms of *modus operandi*) in neighboring countries. Often, perpetrators gradually shift their focus from one country to another. By observing these trends, it is possible to learn from other countries and take appropriate preventive measures to prevent financial losses; this allows for the timely deployment of preventive tools or campaigns to alert citizens to new trends in cybercrime. The structure and format of criminal activity change significantly depending on the popularity of certain web platforms, financial services (tools), or applications.

2.2. Child Abuse and Child Pornography on the Internet

Child abuse and child pornography on the internet are among the most serious forms of cybercrime. Currently, the term “child sexual abuse material” (CSAM) is more commonly used because it better reflects that this is evidence of child sexual abuse, not a legal form of pornography. This is a criminal offense in which information and communication technologies are used to create material depicting child sexual abuse, to distribute, selling, or exchanging such material via the internet; storing or obtaining such material; contacting minors with the intent to sexually abuse them (so-called “grooming”); live streaming of child sexual abuse over the internet, and sextortion—blackmailing a child using intimate photos or videos obtained from them to coerce them into further conduct or payments.

The following tools are necessary for the effective protection of children: educating children on the safe use of the internet (lectures at various educational levels and on various platforms—both online and in person), parental supervision and open communication (adequate public awareness is necessary), adjusting privacy settings on social media (national legislation, user

protection on private networks, and the like), caution when communicating with strangers (working with children of all age groups starting from an early age), and immediately reporting suspicious content or behavior to the relevant authorities or the service provider (followed by the adjustment of notification mechanisms, and so on).

Perpetrators often operate across the borders of multiple countries; detecting this criminal activity requires close cooperation among national law enforcement agencies, international organizations, and internet service providers in identifying perpetrators, removing illegal content, and protecting victims.

A key organization in this field is the National Center for Missing & Exploited Children (NCMEC)—a nonprofit organization whose mission is to protect children from abduction, sexual abuse, human trafficking, and other forms of exploitation, including crimes committed online. NCMEC works closely with law enforcement agencies, technology companies, nongovernmental organizations, and international partners to prevent, detect, and investigate crimes committed against children.

CyberTipline—one of NCMEC’s most important tools is the CyberTipline, a national reporting system for cases involving child sexual abuse material (CSAM), online grooming, sexual exploitation of children, child trafficking, online solicitation of children for sexual purposes, and other forms of online abuse.

Information is provided by members of the public, electronic communications service providers, social media operators, cloud service providers, and other companies offering internet-related services. NCMEC then analyzes the reports and forwards them to the appropriate law enforcement agencies.

NCMEC provides analytical support (data) to investigators, assists in identifying victims of sexual abuse (though the data is often limited), supports the search for missing children, coordinates among law enforcement agencies (linking cases—though the data is often limited as well), and digital analysis of visual materials.

NCMEC collaborates with major online service providers who are legally required to report instances of detected child sexual abuse material. For example, it works with Google, Meta Platforms, Microsoft, Apple, and other providers of electronic communications and cloud services.

NCMEC works closely with organizations such as Europol, Interpol, INHOPE, national police forces, and national hotlines for reporting illegal content. This collaboration is crucial because online child sexual exploitation is often cross-border in nature and requires a coordinated international response. NCMEC is considered one of the world's leading organizations in the field of protecting children from online sexual exploitation. Through its CyberTipline system, it receives millions of reports annually from internet service providers and the public, thereby significantly contributing to the identification of victims, the detection of perpetrators, and the support of criminal investigations at both the national and international levels.

Practical recommendation

Establish sufficient capacity within law enforcement agencies, ensuring that personnel have the appropriate training and experience to review NCMEC reports. In terms of volume, this involves a large number of reports with varying formats and data specifications. These must be thoroughly analyzed and verified (using analytical tools—OSINT) to identify the perpetrator—and the investigation must then proceed.

It is also essential to ensure the flow of information within police structures to ensure sufficient promptness in investigating serious reports (involving multi-level police cooperation within the investigation, possible collaboration with the private sector, and so on—to secure digital evidence across various platforms, as perpetrators typically use external or cloud services for data storage).

2.3. Online Radicalization and Terrorism-Related Content

Online radicalization and terrorism-related content pose a significant security threat, as the internet and social media enable the rapid spread of extremist ideologies, propaganda, and instructions for committing acts of violence. Radicalization is a process in which an individual gradually adopts extremist views that may lead to supporting or committing acts of violence to advance political, religious, or ideological goals.

The internet greatly facilitates this process through social media, discussion forums, encrypted messaging apps, video platforms, online communities, and closed groups (including chat rooms in online games). Perpetrators or extremist groups often exploit social media algorithms, the anonymity of the internet, and the targeted outreach to vulnerable individuals.

Content related to terrorism is defined as material that promotes or glorifies terrorist acts, incites the commission of terrorist crimes, encourages support for or recruitment into terrorist organizations, provides instructions or training on how to carry out terrorist attacks, or disseminates violent extremist propaganda with the aim of radicalizing others. Typical forms of dissemination include social media posts, videos and live streams, e-magazines and leaflets, podcasts, encrypted communication channels, websites, and discussion forums.

Prevention and the fight against radicalization. This includes, for example, monitoring publicly available extremist content in accordance with the law, removing illegal content from online platforms, education in media and digital literacy, promoting critical thinking, and international cooperation among law enforcement agencies and online service providers. Europol (European Counter Terrorism Center—ECTC), Interpol, the European Union, the Council of Europe, and the United Nations play a significant role in the fight against terrorism and online radicalization. These organizations support the exchange of information, the coordination of investigations, and the removal of illegal content from the internet.

Practical recommendation

Establish sufficient capacity and communication links between cybercrime units and counterterrorism units. The online environment has a fundamental impact on the spread of radical theories and has become a mass communication platform. Mutual cooperation is also necessary between police units (including Europol's national headquarters), government institutions, and the media. Last but not least, efforts must also be made at the educational level (from elementary school through higher education), where there needs to be active discussion about the activities and forms of radicalized groups, as well as their hidden manifestations. Intensive cooperation among all relevant bodies is essential, as the rise of radical or extremist expressions in the online environment is a major concern.

2.4. Broader risks associated with digital platforms and the use of social media (threats, defamation, personal attacks/threats to personal status, etc.)

Broader risks associated with digital platforms and the use of social media represent a significant social problem. While social networks, discussion forums, and communication apps facilitate communication and the sharing of information, they can also be misused to commit illegal or harmful activities.

Main risks:

Cyberbullying—this involves the repeated harassment, ridicule, or intimidation of a person via the internet or digital technologies. It can take the form of offensive messages, the publication of humiliating photos or videos, or the creation of fake profiles.

Slander and Defamation – the dissemination of false or misleading information can damage an individual's personal or professional reputation. Such conduct may have both civil and criminal consequences, depending on the circumstances.

Personal attacks and hate speech—users may be targeted with insults, threats, or hate speech based on their nationality, ethnic origin, gender, disability, religion, or other characteristics. In some cases, this may constitute a criminal offense.

Doxxing—this involves the unauthorized disclosure of personal information (such as an address, phone number, or place of work) with the intent to intimidate, harass, or endanger a specific person.

Identity theft—attackers can obtain users' personal data from social media and misuse it to create fake profiles, commit fraud, or gain unauthorized access to accounts.

Disinformation and manipulation—digital platforms enable the rapid spread of false or misleading information that can influence public opinion, trust in institutions, or citizens' decision-making.

Online Stalking (Cyberstalking)—This involves the prolonged monitoring, harassment, or intimidation of a person through electronic communication, often accompanied by threats or unsolicited contact.

Privacy violations—users may unintentionally disclose sensitive information, photos, or location data, which can then be misused.

Manipulation and social engineering—attackers use psychological techniques to obtain confidential information or persuade the victim to perform certain actions (such as sending money or providing login credentials).

Social media addiction – Excessive use of digital platforms can negatively impact mental health, interpersonal relationships, work performance, or academic performance.

These risks can lead to mental health issues (anxiety, stress, depression), damage to one's reputation, financial loss, invasion of privacy, loss of trust in digital services, social isolation, or conflict.

To reduce risks (as a preventive measure), it is advisable to protect personal data and share it only to the extent necessary, use strong and unique passwords along with multi-factor authentication, regularly check privacy settings on social media, critically verify information before sharing it, refrain from responding to provocative or hateful posts, and use the options to block or report users; preserve

evidence (screenshots, messages) in cases of harassment or threats; and, if necessary, contact the platform operator or law enforcement authorities. Responsible use of digital platforms, the development of media and digital literacy, and adherence to principles of safe online behavior are among the most effective tools for preventing these risks.

Practical Recommendations

Establish communication and information-sharing mechanisms between cybercrime police units and prevention units (communications and prevention). Adequate public awareness campaigns and the sharing of information about potential threats related to this issue are necessary. Mass media and other communication channels should be involved in preventive measures to the greatest extent possible. Government and educational institutions should also be involved, particularly in raising awareness among children and youth. Actively respond through police communication channels (Facebook, Instagram) to current threats and situations that could endanger youth or specific groups (in the case of specifically targeted activities or campaigns). Official social media accounts of police departments (Facebook, Instagram) appear to be the most effective tool for sharing information and alerts (due to their large following among residents of all age groups).

Practical Examples / Prevention Tools

Safe online/reporting platforms and tools for children (involving both the private and public sectors)

A safe online environment for children requires cooperation among government institutions, law enforcement agencies, schools, nongovernmental organizations, and commercial technology companies. The goal is to prevent cyberbullying, online sexual abuse, fraud, and other forms of online threats to children. Every form of threat to children and adolescents must fall under the jurisdiction of a specific government agency. I recommend establishing commissions with representation from the relevant ministries (Interior, Education, Family, and others as appropriate) and developing a comprehensive program for the protection of youth. Non-governmental organizations active in this field can also provide significant assistance in this matter (particularly regarding experience with reporting incidents—web interfaces, hotlines, and other methods)—drawing on the experiences of other countries or transnational and European projects.

Government reporting and support platforms:

The Police Force of the Slovak Republic

- receives reports of criminal activity on the internet,
- investigates cases of cyberbullying, fraud, grooming, and child sexual abuse
- provides preventive information on safe internet use (recommended Facebook and Instagram channels)
- and collaborates with other ministries and non-governmental organizations to develop preventive tools, reports, alerts, and similar resources

National Cyber Security Center

- receives reports of cyber incidents,
- issues security recommendations (primarily regarding vulnerabilities in information infrastructure, specifically targeted attacks, and campaigns exploiting specific hardware and software vulnerabilities)
- alerts the public to current cyber threats (in cooperation with the private sector, it publishes alerts regarding specific types of threats, attacks, or targeted campaigns against platforms, payment interfaces, tools, and the like)

National Helpline for Children at Risk (24/7 hotline)

- provides anonymous assistance to children,
- offers consultations regarding cyberbullying or online harassment,
- offers guidance to parents, schools, and specific entities that have been targeted by an attack

International Platforms

INHOPE – brings together national hotlines for reporting child sexual abuse material (CSAM) and ensures its referral to the appropriate authorities.

Europol – supports investigations into international cybercrime and coordinates cooperation among member states to protect children online.

Interpol – collaborates to identify victims and perpetrators and dismantle international networks involved in child sexual abuse.

Involvement of Commercial Companies – Several large corporations are actively involved in protecting children from online abuse. These are typically companies that are active in this field. Part of this collaboration involves coordinating efforts with the police and other government agencies to implement preventive measures or reporting tools. This may include reporting any harmful or inappropriate content.

Examples -

- Google – reporting inappropriate content, the Family Link feature, and SafeSearch.
- Meta (Facebook and Instagram)—reporting users, blocking accounts, parental controls, and privacy protection.
- TikTok – Family Pairing, screen time limits, and content reporting.
- YouTube – YouTube Kids, parental controls, and a video reporting system.
- Microsoft – Family Safety for managing screen time, content filtering, and monitoring
- children's safety.

By communicating with these entities and by properly and effectively assigning responsibility at the national level, it is necessary to establish effective and responsive mechanisms for identifying inappropriate content or victims. Subsequently, appropriate measures must be taken by all responsible departments and institutions.

Safety Tools for Children and Parents

Most commonly used measures:

- parental controls on devices,
- filtering of inappropriate content,
- time limits on internet use,
- monitoring of downloaded apps,
- privacy settings on social media,
- two-factor authentication for user accounts,
- regularly updating devices and apps.

The Role of Schools and Parents

Effective protection of children requires:

- digital literacy education,
- the development of critical thinking,
- open communication between children, parents, and teachers,
- support for reporting inappropriate behavior,
- the creation of a safe online environment.

Practical recommendation

Protecting children online relies on cooperation between the public and private sectors. Government agencies are responsible for investigating and preventing criminal activity, while technology companies can provide tools for reporting inappropriate content, parental controls, and privacy protection. Schools, parents, and children themselves also play an important role; they should know how to recognize risky situations and not be afraid to report them. This awareness depends heavily on the preventive measures implemented by all involved parties.

Awareness-raising initiatives for various groups (seniors, citizens/parents, educators, etc.)

Raising awareness of cybersecurity is one of the most effective tools for preventing cybercrime. Educational and preventive activities are tailored to different population groups based on their needs and level of digital literacy.

Initiatives for Seniors

Seniors are among the groups most frequently targeted by online scams and social engineering. Prevention programs should focus on:

- recognizing phishing emails, text messages (smishing), and phone scams (vishing),
- the safe use of online banking,
- protecting personal data and passwords,
- safe online shopping,
- verifying the credibility of websites and online offers.

Education should be provided through lectures, workshops, information campaigns, and practical demonstrations.

Any sector can participate in these activities.

Initiatives for Citizens and Parents

The goal is to raise awareness of the risks of the internet and provide parents with tools to protect their children. Programs should focus on:

- safe use of social media,
- cyberbullying and online harassment,
- parental controls on devices,
- privacy and personal data protection,
- prevention of online fraud,
- and recognizing misinformation.

Parents should be encouraged to communicate openly with their children about their online activities.

Initiatives for Educators

Educators play a key role in building a safe digital environment in schools. Training should include:

- cyberbullying prevention,
- recognizing risky behavior among students,
- protection of personal data in the school environment (networks, interfaces, applications, etc.)
- safe use of digital technologies in the classroom,
- procedures for handling cyber incidents (starting with simple ones)

This should include methodological materials, training sessions, and professional seminars. Responsibility and initiative lie with the relevant government agency.

Initiatives for Children and Youth

Programs should be tailored to children's ages (and digital literacy) and focus on:

- safe online behavior,
- protection of personal data,
- recognizing online manipulation,
- prevention of grooming and sexting,
- safe use of social media (with an emphasis not only on one's own personal information and data)
- critical evaluation of information and the development of media literacy.

Training should be conducted through interactive workshops (most effective), age-appropriate simple games, contests, and e-learning courses.

Initiatives for Organization Employees

Organizations can conduct regular training activities in the following areas:

- information and cybersecurity,
- recognizing phishing attacks and campaigns,
- safe use of work devices (with regard to corporate interfaces and applications),
- protection of sensitive data,
- secure remote work (remote management, cloud solutions, and access to services).

Simulated phishing campaigns can also be used to test employees' preparedness.

Targeted approaches to informing and raising awareness (law enforcement agencies, courts, and prosecutors' offices).

Effectively combating computer and cybercrime requires not only modern technologies but also ongoing training and the enhancement of professional competencies among staff at , law enforcement agencies, the prosecutor's office, and the courts. The goal is to ensure a uniform,

effective, and lawful approach to the prevention, detection, investigation, and adjudication of cybercrimes. Information should focus primarily on current and emerging trends, modus operandi, vulnerabilities of specific groups, and similar topics.

Law Enforcement Agencies – LEA

Training Areas

- investigating cybercrimes (procedures, advice, etc.)
- Securing and analyzing electronic evidence (options and scope of forensic examinations),
- investigating online fraud, ransomware attacks, and unauthorized access to information systems (availability of tools, cross-sector IT collaboration),
- use of open-source intelligence (OSINT—cooperation with Europol, the commercial sector, training activities),
- international police cooperation (and beyond),
- protection of victims of cybercrime (preventive measures and solutions).

Types of Education

- professional training and courses,
- practical exercises and incident simulations,
- international conferences,
- exchange of experiences among police forces,
- e-learning programs.

Prosecutor's Office

- legal classification of cybercrimes (under both local and European legislation),
- evaluation of electronic evidence (including its collection from abroad),
- international judicial cooperation,
- application of international conventions and European Union law,
- protection of the rights of victims and witnesses.

This training helps ensure consistent practices in the prosecution of computer crime.

Courts

Judges must be prepared to rule on technically complex cases that often involve digital evidence and international aspects.

Key areas of training:

- evaluation of electronic evidence,
- digital forensics and its limitations,
- legal issues related to privacy and personal data protection,
- international judicial cooperation and its possibilities,
- current case law in the field of cybercrime.

Targeted information sharing and awareness-raising among law enforcement agencies, prosecutors' offices, and courts are essential prerequisites for successfully combating cybercrime. Ongoing professional training, the exchange of experiences, and international cooperation enhance the state's ability to respond to new forms of cyber threats and ensure the effective protection of citizens' rights in the digital environment.

Conclusion

Effective prevention of cyber threats is based on multisectoral cooperation that brings together public administration, law enforcement agencies, the judiciary, the academic community, civil society organizations, the private sector, the media, and citizens themselves. Key elements include systematic education, the development of digital and media literacy, effective incident reporting mechanisms, information sharing, and a coordinated response to emerging threats. Such an approach strengthens society's resilience against cyberattacks and contributes to a secure and trustworthy digital environment.

3. Building Sufficient or Adequate Capacities to Combat Cybercrime

Recommendations:

- developing personnel capacity with sufficient technical equipment and security measures (adequate training for police officers specializing in this field, technical equipment—both hardware and software—as well as analytical and OSINT tools)
- developing a methodology for investigating cybercrime incidents (+ training for lower-level or subordinate units), making these methodologies available to all police units that may encounter cybercrime cases
- creation of proprietary analytical databases (collection of data from internal investigations, operational data, and data on perpetrators obtained from abroad or other sources)
- establishing a framework for interagency cooperation within the country—defining responsibilities for handling specific incidents, sharing information on cases, and coordinating efforts at both the national and international levels—defining responsibilities and rules
- 24/7 service (availability and coverage for carrying out urgent actions necessary for the investigation—securing electronic evidence)
- Participation in projects of European institutions (use of funds for capacity building)

Expectations:

- Increased use of anonymization techniques by perpetrators—strengthening and building capacity (TOR, VPN, torrent, peer-to-peer, etc.)
- an increase in the number of cases (capacity building across police units at all levels of management)—changes in the forms and applications of modus operandi
- GDPR – complications regarding the availability of data, reduced ability to secure data from commercial sector entities – solutions: more intensive cooperation, identifying areas of overlap, opportunities for mutual cooperation and sharing of “know-how,” joint educational and preventive activities