AGORA International Journal of Juridical Sciences, http://univagora.ro/jour/index.php/aijjs
ISSN 1843-570X, E-ISSN 2067-7677
Vol. 19, No. 2 (2025), pp. 20-41

INTERNATIONAL JUDICIAL COOPERATION IN THE CONTEXT OF THE ADOPTION IN 2024 BY THE UNITED NATIONS OF THE CONVENTION ON CYBERCRIME

M.D. BOGDAN

Manole Decebal Bogdan
Faculty of Law and Social Sciences, "December 1, 1918 " University of Alba Iulia, Romania
https://orcid.org/0000-0001-8662-1243, E-mail: decebal.bogdan@uab.ro

Abstract: *The practical application of the United Nations Convention against Cybercrime requires complementarity in the reactions of states or state unions to new opportunities for perpetrators of cybercrimes that are extremely dangerous for societies and the global economy. The application of the Convention strengthens the mechanisms for preventing and combating crimes in the digital space, but judicial cooperation must be based on a series of efficient procedures, in the context in which geographical territoriality is substituted by the fluidity of the virtual space of the Internet, sometimes without clear jurisdiction.*
Keywords: *International judicial cooperation, Cybercrime, Cybersecurity procedures; cyber protection; UN convention of 2024*; Advanced persistent threat – APT.

1. Introduction to the research topic

Digital developments in parallel with artificial intelligence tools have determined the need for a scientific technology of the phenomenon but also a pragmatic approach to coercive measures to limit the effects of crime in cyberspace. The effects of cybercrime are felt in society every day. The tools used by criminals through cybercrime are modernized and optimized so that victims generate as many effects with the highest values as possible. Cybersecurity is one step behind cybercrime although it is coordinated by the special structure of the state authority. In reality, conflicts between countries, even friendly ones, are also extended through the cybercrime procedure. We usually define the perpetrators as "state actors". The product of cybercrime is recycled. In this context, state administrations must find a common path of international cooperation on judicial procedures to combat the phenomenon of cybercrime.

Preventing and combating cyber activity and the criminal responsibilities of all states! Cybercrime manifests itself in a parallel space with society, called virtual space.

" *No country is an island: embracing international law enforcement cooperation to reduce the impact of cybercrime [John Billow , 2024], Head of the National Cyber Security Center (NCSC-SE) in Sweden and former official at the Interpol Cybercrime Directorate, with direct experience in international cyber cooperation and operations]".* The expert stated that *"being an inherently transnational challenge, cybercrime requires an international response. John Billow stressed the need for effective collaboration between governments and with the private sector to enforce international law on cybercrime".*

The virtual space of the Internet has no determined constitutional boundaries and jurisdictions. Within this digital space of the Internet there are legal, clear, visible domains. In

the same space there are domains that do not offer transparency on operations, invisible to users without specialization in cyberspace. This space is defined as the " dark internet". " Dark internet [i]" or " dark web" designates that part of the Internet that operates on special networks (darknet), over the public Internet, but accessible only with specific software/configurations (e.g. Tor, I2P) and which is not indexed by regular search engines. In this space there are illegal activities (black markets for drugs, weapons, stolen data, child pornography, hacking services, etc.), but there are also legitimate uses, related to protecting anonymity in repressive regimes or for journalists and activists. The " dark " web is used as an "agora" for cybercrime: forums for coordinating attacks, selling malware, stolen data, custom hacking services [ii]. Criminals operate from a location that is often unknown on the internet space of different countries or unions of countries, but also in international organizational areas, companies, etc. In this context, cybercrime is not always a tactical field of individuals working independently.

Cybercrime also manifests itself through organized groups of professionals in the digital space, in the economic field, in the field of technologies "with support" most often from "state vectors".

In our research, we also took into account the international context created by the Russia-Ukraine conflict. During the conflict period, crime is extremely important. Researchers from Ukraine [iii]in terms of: " *Today, cybercrime and cyberterrorism are identified as one of the threats to the national security of Ukraine in the field of information . committed in cyberspace by computer systems or through the use of computer networks and other means of access to cyberspace, within computer systems or networks, as well as against computer systems, computer networks and computer information, being widely developed. Terms such as "cybercrime", "information crime", "crime in the field of computer information", "crimes in the field of information technology* " have a direct connection with the cybersecurity of the state and information security [Baranenko, Roman. (2021)] .

The importance of the " Dark " web has increased with the active trading of cryptocurrencies. Cryptocurrencies are hosted on virtual servers in " clouds" computing ” through [1]operations that go beyond standard judicial procedures of control exercised by the state.

Countries with treasuries (or reserves) in crypto *:*

El Salvador was the first country to adopt Bitcoin as legal tender (2021) and integrated it into its national financial strategy, treating it as a sovereign reserve asset. In 2025, it had over 7,500 BTC in its state portfolio, managed for the long term.

The United States has the largest government stockpile of Bitcoin , mainly from seizures in cybercrime cases; some is now managed under a "Strategic Bitcoin" framework. Reserve ”. Recent estimates range from around 28,000 BTC (in US Marshals custody) to several hundred thousand BTC at the federal supply level.

Other countries with notable Bitcoin holdings *China* – reserves estimated at around 190,000 BTC, mainly from the PlusToken scheme seizure ; treated as state assets, even though there is no transparent “ crypto treasury ” policy.

Ukraine, the United Kingdom, Bhutan, the United Arab Emirates, Venezuela, Finland – appear on the charts with government holdings of Bitcoin , through confiscations, state mining, or one-off measures.

[1]Not all holdings = “treasury” policy. In many cases, cryptocurrencies are held by the state as a result of confiscations rather than as a result of a treasury investment decision (e.g. US, China, UK). El Salvador remains the clearest example of a state using Bitcoin as an explicit sovereign reserve asset in its financial strategy.

Examples of sub-national "treasuries" (USA): Some US states (e.g. New Hampshire, Texas, Arizona, Oregon) have passed laws that allow or require the establishment of reserves in Bitcoin or other digital assets, managed by state treasuries. New Hampshire, for example, authorizes the treasurer to invest up to 5% of public funds in very large-cap digital assets (basically Bitcoin).

2. Cybercrime is a global threat

There is a lot of research on cybercrime, especially from information technology specialists in the virtual space of the Internet. The product of cybercrime affects the entire society because the scope of action is not limited by state border control. Cybercrime affects the state and society vertically: critical state infrastructures become difficult to manage and control; sensitive information of political power is stolen by state actors (friends or enemies); military command structures become vulnerable; the structure regarding the administration of personal data or data regarding the health status of the population is subject to the risk of theft, so Cybercrime is also manifested in the manipulation of the population in the electoral mechanism.[iv] [Georgiana PETRE-FRISCHHERZ, *Technology in Election Campaigns, 2025].* This issue raises serious issues regarding the sovereignty of states and the inability not to protect against external attacks from states interested in the constitutional order of Romania. In this vein, we also find the concern of the diplomat [v]from the United States of America who appreciates: *"The global landscape has an evolution that accelerates international events and requires the pace of increasingly nuanced diplomatic actions."* The United States Department of State has said [2]it is appropriate to " *coordinate with diverse state and non-state actors, with their own interests, given relationships. The digital age presents an extraordinary opportunity to share information and connect across historical divides. and promote antidemocratic agendas. To counter these trends, U.S. diplomacy must be multifaceted and encompass a wide range of issues, such as human rights, economic initiatives, and security assistance. U.S. diplomacy must be cross-functional , nuanced, and rapid, delivering results for its people in the pace of global events."*

Researchers believe that:

- ✓ *Ransomware is a threat to peace and security: understanding and avoiding the worst-case political scenarios* [Mischa Hansel and Jantje Silomon , 2024]. The authors analyze three scenarios in which ransomware could escalate political tensions and identify the structural factors driving these risks and highlight the urgent need for global institutional solutions to address the widespread consequences of ransomware. The frequency and severity of ransomware attacks raise questions about their potential classification as cyberterrorism [vi]. [Lora Pitman and Wendy Crosier , 2024] examines large-scale incidents such as the Colonial

[2] *Enterprise Data Strategy – Empowering Informed Data Diplomacy, September 2021* , Department of State, United States of America, https://www.state.gov/wp-content/uploads/2021/09/Reference-EDS-Accessible.pdf

Pipeline attack [3]and wiperware attacks. [4]against Ukraine in 2022, to explore how ransomware affects national and global security. The authors proposed a new framework for determining when ransomware constitutes cyberterrorism , addressing the lack of consensus among researchers and policymakers. The authors emphasize the importance of a clear definition to guide policy responses and highlight the implications of their findings for national strategies and UN-level negotiations on cybercrime.

✓ *We find [vii]that a new discipline, Cyber Criminology, has developed to study the causality of crimes that occur in cyberspace and the impact on physical space. Understanding cyberspace is a necessity in analyzing the empirical and theoretical aspects of cybercrimes, cybercriminal behavior, cybervictims, cyberlaw, and cyberinvestigations.* [Issac, Reji. (2011). Application of cybernetics in cybercriminology. 10.13140/RG.2.1.4263.6565.]

✓ *The greatest challenge is not the distant future dominated by advanced technologies, but the revolutionary changes that are already impacting everyday life [viii]*[Hunter, Albert, Rutland et al. 2024].

The reaction of the international community to the phenomenon of crime in cyberspace and the development of the Convention under the authority of the United Nations. The international community found that the phenomenon cannot be controlled. The evolution and size of potential damage were monitored in terms of: economic, political, industrial and military. The interference between society and the digital space is increasing.

Whoever dominates cyberspace will dominate the real world. In the real world, society is dependent on cyberspace through voluntary connection to social media networks and commercial platforms – economic ones, *etc. in electronic form on serious crimes"* which we define in the presentation of the material as ***"the Convention".*** The Convention criminalizes a limited number of crimes facilitated by digital technologies at the same time as the core cybercrimes. The Convention applies, in situations of *"Prevention, investigation and prosecution of stability crimes under the Convention, including the freezing, seizure, confiscation and return of the proceeds of such crimes".* It also falls under the scope of the Convention " *Collection, obtaining, preservation and sharing of evidence in electronic form for the purposes of criminal investigations or proceedings* " [article 3]. States Parties to the Convention shall ensure that stability crimes in accordance with these conventions and protocols are also considered as crimes under their domestic law when committed through the use of information and communication technology systems . In accordance with the Convention, no provision shall be interpreted " ***as establishing criminal offences"*** .

[3]On May 7, 2021, Colonial Pipeline shut down its operations after a ransomware attack on its IT systems by the criminal group DarkSide. The shutdown disrupted fuel supplies along the East Coast, causing panic buying, long lines at gas stations, and localized price increases, as well as impacting the availability of jet fuel. Colonial paid the attackers approximately $4.4 million in cryptocurrency; U.S. authorities later recovered approximately $2.3 million of this amount. The incident prompted major discussions and policy action on increasing cybersecurity for critical infrastructure in the United States. [https://www.energy.gov/ceser/colonial-pipeline-cyber-incident]

[4]wiper attacks began in January 2022, before the full-scale invasion on February 24, targeting Ukrainian government institutions and critical infrastructure. cyber.[https://www.aha.org/cybersecurity-government-intelligence-reports/2022-02-26-tlp-white-joint-cyber-advisory-destructive]

Researchers also have different opinions towards the legislator and appreciate [ix]: " *Cyber investigations can be invasive, and digital rights groups argue that the scope has expanded and the lack of sufficient guarantees puts human rights at risk ."*

Although the area of manifestation of cybercrime is international, the Convention, through Article 5, prohibits states from exercising, in the territory of another state, jurisdiction and performing functions that are reserved exclusively to the authorities of that other state by its internal law. It states that the principles of sovereign equality and territorial integrity of states and the principles of non-interference in the internal affairs of other states are respected.

An important part of the "Convention" is that its provisions cannot be interpreted as permitting the suppression of human rights or fundamental freedoms, including the rights related to expression, conscience, opinion, religion or belief, peaceful freedom and association. The "Convention" is drafted in accordance with and in a manner compatible with applicable international law in the field of fundamental human rights.

Our research proposes to find points of reference for debates, ideas and starting points in a solution found to the challenges of cybercrime. For the European Union, the "Council" has developed *Council Decision (EU) 2025/2307*[x] with the aim of strengthen international cooperation in combating certain crimes committed by means of information and communication technology systems and for the exchange of electronic evidence in relation to serious crimes. The speed with which the Convention was adopted demonstrates that the European Union has had a significant voice from the very beginning of the implementation of this new global framework for combating cybercrime. The conclusion of the Convention by the Union does not affect the competences of the Member States to ratify, accept or approve the Convention, in accordance with their internal procedures. The Member States retain competence in so far as the Convention does not affect common rules or alter their scope [xi].

3. Regulations and judicial procedures regarding cybersecurity in Romania

The Convention does not conflict with the domestic law of the states nor with the legislation on combating cybercrime. Romania has developed a specific legislation on cybercrime as the legal relationships between perpetrators/criminals and society have become increasingly evident, and the phenomenon of crime has become ineffective due to the lack of clear legal provisions in criminal legislation. Investigative authorities have resorted to classifications and assimilations of the acts to be incriminated. Romania has developed **a complex regulatory framework for regulating and combating cybercrime .**

The legislative framework is composed of multiple legislative layers covering both the criminalization of illicit acts committed in cyberspace, as well as prevention measures, cybersecurity and international cooperation. Our analysis is carried out separately on *Primary Legislation* (A) and *Secondary Legislation (B)* , Cyber Security Legislation (C), as follows:

A. Primary Legislation – Criminal Code Offenses Regarding Cybercrime

The Penal Code (Law no. 286/2009), amended by Law no. 187/2012 (entered into force on 1 February 2014), **took over the previous computer crimes regulated** in Law 161/2003 and Law 365/2002 **,** concentrating them in Title VII, Chapter VI in Articles 360-366 [xii,xiii]

A.1. Crimes against the security and integrity of computer systems and data

1. **Illegal access to an information system (art. 360 CP)**
- Simple form (paragraph 1): unauthorized access to an information system – punishment: 3 months-3 years imprisonment or fine
- Aggravated form (paragraph 2): access for the purpose of obtaining computer data – punishment: 6 months-5 years imprisonment
- Qualified forms (paragraph 3): when it targets government or military systems or causes significant damage – the punishment is increased by one third

2. **Illegal interception of computer data transmission (art. 361 CP)**
- Unlawful interception of a non-public computer data transmission
- Punishment: 1-5 years in prison

3. **Alteration of the integrity of computer data (art. 362 CP)**
- Modifying, deleting, damaging computer data or restricting access to it, without right
- Punishment: 1-5 years in prison
- This offence transposes art. 4 of the Budapest Convention and art. 5 of EU Directive 2013/40

4. **Disruption of the functioning of information systems (art. 363 CP)**
- Serious, unauthorized disruption of the functioning of the computer system by entering, transmitting, modifying, deleting or damaging data.
- Punishment: 2-7 years in prison
- Covers DDoS and ransomware attacks

5. **Unauthorized transfer of computer data (art. 364 CP)**
- Unauthorized transfer of data from a computer system or storage medium
- Punishment: 1-5 years in prison

6. **Illegal operations with computer devices or programs (art. 365 CP)**
- Paragraph (1): Production, import, distribution, sale of devices, computer programs, passwords, access codes intended for the commission of crimes under art. 360-364 – punishment: 6 months-3 years imprisonment or fine
- Para. (2): Unlawful possession of these instruments – punishment: 3 months-2 years imprisonment or fine

7. **Attempt (art. 366 CP)**
- Attempt to commit the crimes under art. 360-365 is punishable

A.2 Economic-financial crimes in the cyber environment

1. Computer fraud (art. 249 CP)
- Entering, transmitting, modifying, deleting computer data, restricting access to or preventing the operation of a computer system, for the purpose of obtaining beneficial material, if damage has been caused.
- Punishment: 2-7 years in prison
- Includes phishing, bank card fraud

2. Carrying out financial transactions fraudulently (art. 250 CP)
- Paragraph (1): Carrying out a cash withdrawal, electronic money loading/unloading, funds transfer operation by using the payment instrument or identification data without consent – punishment: 2-7 years
- Paragraph (2): Execution by unauthorized use or fictitious data – same punishment
- Paragraph (3): Unauthorized transmission of identification data – penalty: 1-5 years

Jurisprudence of the HIGH COURT OF CASSATION AND JUSTICE regarding the use of bank cards:
- Installing skimmers /cameras at ATMs = crime under art. 365 of the Criminal Code (illegal operations with devices)
- Using the authentic card without the holder's consent = art. 250 para. (1) CP
- Using a counterfeit card = art. 250 + art. 313 CP (according to the real one)
- Using contactless without permission = art. 360 + art. 250 CP (agreed)

3. Illegal operations with non-cash payment instruments (art. 250[1] CP)
- Criminalizes the counterfeiting, possession, trafficking of electronic payment instruments

4. Acceptance of fraudulent financial transactions (art. 251 CP)
- Punishment: 1-5 years in prison

5. Computer forgery (art. 325 CP)
- Unauthorized insertion, modification, deletion of computer data or restriction of access, resulting in data in question
- Punishment: 1-5 years in prison
- Includes falsification of electronic documents, manipulation of databases

A.3 Crimes against the person in the cyber environment

Child pornography (art. 374 CP)
- Producing, possessing, distributing, applying, presenting pornographic materials with minors through computer systems
- Qualified forms: when the victim is exploited, when the member of the organization, when injury/death resulted
- Automatic entry into the competence of DIICOT, regardless of the existence of an organized criminal group

B. Special Legislation on the Prevention and Combating of Cybercrime

B.1. Law no. 161/2003[xiv] regarding some measures to ensure transparency in the exercise of public dignities, public functions and in the business environment, the prevention and sanctioning of corruption is defined in Book I - *General regulations for the prevention and combating of corruption.* Title III surprises – *Preventing and combating cybercrime* (articles 34-66) regulates the framework for prevention, definitions and cooperation.

1. Fundamental definitions. In art. 35 of the law are defined: **Information system** : device or set of interconnected devices that ensure automatic data processing**; Information data** : representation of facts, information or concepts in a form processable by an information system; **Service provider** : natural/legal persons that provide communication through information systems or store/process data; **Data related to information traffic** : data about origin, destination, route, time, date, size, volume, duration of communication; **Security measures** : procedures, devices, specialized programs for restricting/prohibiting access; **Unlawful action** : lack of legal/contractual authorization, exceeding limits, lack of permission .

2. Preventive measures. The law establishes in (art. 36-41) preventive activities of public communes, public joint activities, service providers, NGOs, information campaigns (Art. 36-38). Regarding preventive measures regarding computer crime of databases, responsibility is given to the Ministry of Justice, the Ministry of Internal Administration, the Ministry of Education and Research, the Romanian Intelligence Service and the Foreign Intelligence Service (Art. 39). In article Art. 40 are defined prevention measures through *special personnel training programs,* and Art. 41 specifies the obligation of owners/administrators of systems with restricted access to warn users about the consequences of unauthorized access (warning accessible to any user) .

3. Contraventions (art. 52-53) for Failure to comply with the warning obligation (art. 41) = contravention, fine: 5,000-50,000 lei) .

4. International cooperation in (art. 60-66) refers to The establishment of **the Cybercrime Combating Service** in the Prosecutor's Office attached to the High Court of Cassation and Justice as **a permanent contact point** available 24/7 with: Specialized assistance, legislative

data; Immediate data preservation at the request of foreign authorities; Execution of letters rogatory. Art. 63-64 define the procedure for immediate preservation of computer data at international request (min. 60 days)

Important note : Articles 42-51 (specific offenses) were repealed on February 1, 2014 by Law No. 187/2012 and transferred to the Criminal Code.

B.2 Law No. 365/2002 on electronic commerce . It regulates electronic commerce and previously provided (art. 24-28) for crimes related to electronic payment instruments. These articles have been partially repealed and integrated into the Criminal Code.

C. Special Legislation for Cyber Security

C.1 Law no. 58/2023 on the Cybersecurity and Defense of Romania , Entered into force on March 14, 2023, the framework law for cyber security and defense at the national level [xv]. By Government Decision no. *1321/2021, the Cybersecurity Strategy of Romania* [xvi]was approved , *for the period 2022-2027, as well as the Action Plan for the implementation of the Cybersecurity Strategy of Romania* , for the period 2022-2027.

1. Institutional framework (art. 6-19). National Cyber Security System (SNSC) – general cooperation framework coordinated at the strategic level by **the CSAT** and at the operational level by the **Cyber Security Operational Council [5](COSC)** .

Responsibilities : harmonization of responses to cyber threats, recommendations on alert levels, international cooperation, action plans

Competent authorities (art. 10-18):

- **National Cyber Security Directorate [xvii](DNSC)** : authority for **the national civil cyberspace** (art. 10 letter a)
- **MCID** : development of normative acts, public policies in the field of cybersecurity, digital transformation (art. 10 letter b)
- **National Authority for Administration and Regulation in Communications [xviii](ANCOM)** : coordination of cybersecurity of networks and information systems of electronic communications providers (art. 10 letter c)
- **Ministry of Internal Affairs [xix](MAI)** : knowledge, prevention, identification, countering threats, vulnerabilities, cyber risks (art. 12)
- **Romanian Intelligence Service [xx](SRI)** : **cyber intelligence** and prevention/counteraction **of APT** (Advanced Persistent Threat) against national security (art. 14); residual attribution for APT in all cases not covered by other authorities
- **Ministry of National Defense [xxi](MApN)** : **cyber defense** , defensive/offensive cyberspace operations, military cyber intelligence/counter-intelligence (art. 11, 30)
- **Foreign Intelligence Service [xxii](SIE), Special Telecommunications Service [xxiii](STS), Guard and Protection Service [xxiv](SPP), Office of the National Register**

[5]The Cyber Security Operational Council (COSC) (art. 8-9) is a consultative body without legal personality, under the coordination of the Supreme Council for National Defense (CSAT). The members of the Supreme Council for National Defense are: the Minister of National Defense, the Minister of National Affairs, the Minister of Foreign Affairs, the Minister of Justice, the Minister of Economy, the Minister of Public Finance, the Director of the Romanian Intelligence Service, the Director of the Foreign Intelligence Service, the Chief of the Defense Staff and the Presidential Advisor for Security. The Secretary of the Supreme Council for National Defense is appointed by the President of Romania and has the rank of State Advisor within the Presidential Administration.

of State Secret Information [xxv]**(ORNISS)** : cybersecurity of own infrastructures (art. 15-18) .

2. Incident management (art. 20-23). National Platform for Reporting Cybersecurity Incidents [xxvi](PNRISC) – developed and managed by DNSC.

Notification obligations (art. 21):

- Natural/legal persons from art. 3 para. (1) let. b) and c) (electronic communications providers, public service providers): **obligation to notify incidents to PNRISC immediately, but no later than 48 hours** after discovery
- If the information is incomplete: **completion within max. 5 calendar days**
- Authorities with networks art. 3 para. (1) letter a) (defense, public order, national security): notification in compliance with the classified information regime (Criminal Code (Law 286/2009) – art. 249-252, 325, 360-366, 374)

Responsibilities (art. 23): Collection of incident notifications; Evaluation of data and information; Coordination of incident management; Support for remediation of effects; Retention of incident data for **5 years** , without collection of content data .

3. Cyber resilience (art. 24-26)

Proactive measures: Establishing incident response teams (CSIRT). (Computer Security Incident Response Team) is a group of professionals specialized in managing, analyzing and resolving cybersecurity incidents (data breaches, ransomware attacks, etc.). CSIRT is essential for any organization that wants to protect its digital assets. The Cybersecurity Incident Response Team has specialized human resources and a security operations center. In fact, it is a reserve of resources and capabilities that has anticipatory knowledge capabilities on potential threats. Capabilities are also developed through cooperation with the private sector to implement security and/or automatic detection solutions. Other responsibilities are intelligent threat analysis, staff training, awareness campaigns and last but not least, cyber hygiene .

Reactive measures :

- Response and contingency plans
- Use the resource pool
- Restoring functionality
- Broadcast alert
- Deterrence through public attribution of attack perpetrators [1]

The obligations of providers of technical cybersecurity services (art. 25) are to transmit data/information to the authorities within a maximum of **48 hours** (incident) or **5 days** (threats, risks, vulnerabilities).

This is forbidden . requests personal data or content data [1]

4. National Cyber Alert System (SNAC) (art. 27-29)

- **Cyber alert levels** : stability through DNSC methodology, endorsed by COSC
- **Establishment/modification of level** : DNSC director decision, with COSC advisory opinion
- **Obligation** : persons from art. 3 to develop **their own action plans** for each type of alert and to apply them when declaring alert states.

5. Cyber defense – military component (art. 30-31)

The Ministry of National Defense according to (art. 30): Defends and protects its own information systems/networks; Plans and conducts cyberspace operations through the National Military Command Center; Executes peacetime defensive operations through **the Cyber Defense Command;** Develops military capabilities for executing cyberspace operations; Conducts cyber intelligence and cyber counter-intelligence; Develops **offensive response capabilities** , individually or in coalition/alliance, usable in the event of cyberattacks contrary to international law; Participates in cyberspace deterrence activities. **The Ministry of National Defense** is the North Atlantic Alliance (NATO) single point of contact for military cyberspace operations .

6. Supply chain security (art. 41-44)

- **Obligation to manage risks** in the supply chain (fake/counterfeit solutions, fraudulent manipulation, fake components, dangerous services, cyber espionage)
- Designation of cybersecurity responsibility for the chain
- Policies, technical standards, risk assessment, training .

7. Minor offences (art. 48-49)

Art. 48 paragraph (1) – The following acts constitute **contraventions** (if they are not crimes):

a) Failure to comply with the obligation to notify within the incident deadline (art. 21 paragraph 1)

b) Failure to comply with the obligation to fully communicate incidents (art. 21 para. 2, art. 22)

c) Failure to provide data/information by cybersecurity service providers (art. 25 para. 1)

Sanctions (art. 48 para. 2-6):

- **Individuals** : fine **5,000-50,000 lei**
- **Legal entities** : fine **up to 200,000 lei** (for the first offense); for repetition: up to **1% of turnover** (operators >50 employees) or **3% of turnover** (operators >250 employees and >50 million EUR)
- **Finding** : National Cyber Security Directorate (DNSC) and other powers (art. 49)
- **Recipe** : 2 years
- **Appeal** : Bucharest Court of Appeal, within 15 days[xxvii]

8. Related legislative amendments (art. 50-51)

Art. 50 – Amends **Law no. 51/1991 on national security** , introducing: **Lit. n) -** "cyber threats or cyber attacks on information and communications infrastructures of national interest" as **a threat to national security** and **Lit. o) - p) -** resilience to hybrid risks, propaganda/disinformation campaigns in cyberspace [Criminal Code (Law 286/2009) – art. 249-252, 325, 360-366, 374].

Art. 51 – Amends **GEO no. 1/1999** on the state of siege and the state of emergency and includes "cyber defense" in the definition of the state of siege. It also includes *"cyber security for national security reasons"* among the causes of the state of emergency/siege.

There was an obligation to obtain an opinion from the Cyber Security Operational Council (**COSC**), of the Organization and Functioning Regulation course, CSAT Decision No. 17/2013 was approved **when the exceptional measure has cyber security/defense causes .**

C.2 Law No. 362/2018 – Transposition of the NIS Directive (EU Directive 2016/1148) establishes the legal and institutional framework for ensuring a **high common level of security [xxviii]of networks and information systems [xxix]**.

1. Scope

- **Essential service operators** : entities from critical sectors (energy, transport, health, finance-banking, drinking water, digital infrastructure)
- **Digital service providers** : online marketplaces, search engines, cloud computing services

2. Competent authority

- **CERT-RO** (established by Government Decision 494/2011), taken over by **DNSC** by *Emergency Ordinance 104/2021 on the establishment of the National Cyber Security Directorate*[xxx]
- National competent authority, national contact point, CSIRT team [6].

3. Operator and supplier obligations (art. 10-11)

- Cybersecurity **risk management**
- appropriate and proportionate **technical and organizational measures**
- **Incident notification** to CERT-RO/DNSC
- Compliance with technical standards developed by DNSC

4. Minimum security requirements (art. 10 para. 5)

- Rights access management
- User awareness and training
- Activity logging and traceability
- Security testing and evaluation
- Encryption
- Identification and authentication management
- Incident Response
- System maintenance
- Physical protection
- Security plans
- Risk analysis and assessment
- Vulnerability management

C.3 Government Emergency Ordinance No. 104/2021 on the establishment of the National Cyber Security Directorate (DNSC) , which entered into force on September 24, 2021, establishes **DNSC** as a specialized body of the central public administration, subordinate to the Government, under the coordination of the Prime Minister.

1. The DNSC statute is with **legal** entity , fully financed from the state budget.

2. Main responsibility (art. 3): Ensuring cybersecurity **of national civil cyberspace;** Competent national authority for civil cyberspace; Management of cybersecurity risks and incidents [xxxi].

3. Functions and powers (art. 5):

[6]Computer Security Incident Response Team/Cybersecurity Incident Response Team

Strategy and planning : development of strategies, regulations, norms, requirements, guides;
Operations and response : coordination of detection, protection, attack response activities; National *Cyber Security Incident Response Team* ; incident investigation;
National platform for reporting cybersecurity incidents.
Government Cybersecurity Incident Response Team :
Incident response services for public administration.
Certificates : national certification authority in the field of cybersecurity.

- **Registries** : **National Registry of Cybersecurity Assets, Products and Services (RNAPSSC)**
- **Crisis management** : **National Cyber Security Crisis Management Center (CNGCSC)**

C.4. Law no. 163/2021 on information and communications infrastructure of national interest and the conditions for the implementation of 5G networks

Adopted in June 2021, it establishes measures to mitigate security risks, threats and vulnerabilities in the implementation/operation of IT&C infrastructures of national interest.

1. Purpose

- Authorization of manufacturers, distributors, integrators of 5G technologies
- Security risk assessment for critical infrastructure equipment
- Implement **5G Security Toolkit** (EU recommended) [xxxii]

2. Authorization procedure

- MCID submission request
- **CSAT** agenda
- Mandatory CSAT approval for the use of technologies in infrastructures of national interest and 5G networks
- Affidavit: manufacturer/distributor/integrator meets conditions (not subject to foreign government influence, complies with security standards, has no history of security violations)[xxxiii]

3. Authorization withdrawal

- Already authorized technologies can be used **7 years** (general) or **5 years** (network core) after authorization withdrawal

4. Sanctions

- **Offenses** : use of unauthorized technologies in 5G networks
- Immediate ban on use[xxxiv]

Cybersecurity strategies and action plans

1. The Cybersecurity Strategy 2022-2027 established by Government Decision no. **11/2021** is updated according to national/international developments and2 contains a number of five **strategic objectives of strategic importance, as follows:** Action Plan; Secure, resilient networks and systems ; Deterrence and attribution of cyber attacks; Public-private cooperation and Education and awareness[xxxv]

C.6. Directive (EU) 2022/2555 on the security of network and information systems (NIS2)

NIS2 Directive – Non-transposition. was adopted at European level in December 2022, with

the transposition deadline being October 17, 2024 [xxxvi]. Status Romania (December 2025). Transposition has not been carried out. **NIS2 elements** (anticipated to be integrated into future legislation):

- **Scope expansion** : 18 critical sectors (compared to 7 in NIS1)
- **Entity categories** :

○ **Essential** (high criticality sectors): energy, transport, health, public administration, digital infrastructure

○ **Important** (critical sector): postal/courier services, waste management, research

- **More detailed security requirements** : risk management, business continuity, supply chain security, encryption, access controls

○ **Uniform reporting framework** : Early warning - 24 hours; Detailed initial report - 72 hours; Final report with full analysis one month.

- **Stricter sanctions** : up to 4% of turnover or EUR 20 million (compared to 2% in current Romania)
- **Senior management responsibility** : for failure to comply with risk management measures

D Personal Data Protection and Confidentiality of Communications

D.1. General Data Protection Regulation (GDPR/RGPD) [xxxvii]. Regulation (EU) 2016/679 – directly applicable from May 25, 2018 in all EU member states, without the need for transposition.

1. Fundamental principles (art. 5 GDPR): Lawfulness, fairness, transparency; Purpose limitation; Minimization of data used; Accuracy; Storage limitations; Integrity and confidentiality; Responsibility (accountability) .

2. The rights of data subjects are: Right to information; Right of access; Right to rectification; Right to erasure ("right to be forgotten"); Right to restriction of processing; Right to data portability; Right to object and the right not to be subject to automated decision-making [38]

3. The obligations of personal data controllers are:

- Designation **of a Data Protection Officer (DPO)** when mandatory (public authorities, large-scale monitoring, processing of large volumes of special data)
- **Register of processing activities**
- **Data Protection Impact Assessment (DPIA)** for high-risk processing
- **Notification of security breaches** to ANSPDCP within **72 hours**
- Appropriate technical and organizational measures (security by design, security by default)

4. Law stability sanctions are on two levels: Level 1 : up to EUR 10 million or 2% of turnover (global, annual); **Level 2** : up to EUR 20 million or 4% applied to turnover (global, annual) – for serious violations (processing grounds, data subject rights) .

The National Supervisory Authority for Personal Data Processing (**ANSPDCP**) [xxxviii]**is designated as the supervisory authority.**

Law No. 190/2018 on the application of the GDPR Regulation ensures the uniform application of the GDPR in Romania [xxxix]. Main elements : Designation of data responsibility (art. 10); Specific rules for processing for journalistic, academic, artistic, literary purposes: Cooperation with *the National Supervisory Authority for the Processing of Personal Data* .

D.2. The legislation on the protection of privacy in the electronic communications sector establishes specific conditions guaranteeing the right to protection for the protection of privacy in the electronic communications sector **(Law no. 506/2004 [xl])**

1. Prohibition of interception (art. 1 para. 2). Listening, recording, storage, any form of interception/surveillance of communications and traffic data **is PROHIBITED** , with legal exceptions

2. SPAM – Unsolicited commercial communications (art. 12)

- **PROHIBITED** : carrying out commercial communication through automatic calling systems, fax, e-mail, other methods of use, electronic communications services **without the express and prior consent** of the recipient
- **Exception** : if the email address was obtained directly from the customer during the sale of the product/service, for similar products/services, and the customer did not object
- **Message format** : Subject must begin with " **ADVERTISING** " in capital letters
- **Mandatory content** : full name/name, CUI/CNP, domicile/headquarters
- **Right of opposition** : the recipient must be able to request termination in a simple way, free of charge, with effect within a maximum **of 48 hours .**

3. SPAM Sanctions (according to Law 506/2004) for Contravention the sanction is a fine of 5,000-100,000 lei, and for companies with turnover > 5 million lei: fine up to 2% of turnover .

E. Specialized prosecutorial structures for cybercrime of the Public Ministry

E.1 The competence of the Prosecutor's Office in Computer Crime within the structure of the Public Ministry is carried out through offices/prosecutors specialized in computer crimes and the Directorate for the Investigation of Organized Crime and Terrorism Offenses (DIICOT) The Directorate for the Investigation of Organized Crime and Terrorism [xli](DIICOT) carries out criminal prosecution for serious crimes, under the conditions of stability of Emergency Ordinance no. 78/2016 . DIICOT's competence in cybercrime matters (art. 11):

1. Computer crimes that require the existence of an organized criminal group (art. 11 paragraph 1 point 1): **Computer fraud** (art. 249 CP); **Performing fraudulent financial operations** (art. 250 CP); **Illegal operations with non-cash payment instruments** (art. 250[1] CP); **Accepting fraudulent operations** (art. 251 CP); **Computer forgery** (art. 325 CP); **Illegal access to an information system** (art. 360 CP); **Attempting** the crimes listed and highlighted above .

2. Particularly serious computer crimes (>2 million RON) + organized crime group (art. 11 paragraph 1 point 2): Computer fraud, fraudulent financial operations, computer forgery (if the damage is >2,000,000 RON) .

3. Computer crimes that AUTOMATICALLY fall within the competence of DIICOT (art. 11 paragraph 1 point 2): **Illegal interception** (art. 361 CP); **Alteration of data integrity** (art. 362 CP); **Disruption of the functioning of systems** (art. 363 CP); **Unauthorized data transfer** (art. 364 CP); **Illegal operations with devices/programs** (art. 365 CP); **Child pornography** (art. 374 CP); **Attempt** to commit crimes 361-365

4. The competent court is the Court of First Instance for cases under DIICOT jurisdiction .

Note : **NOT all cybercrimes automatically fall under the jurisdiction of DIICOT** . For example, illegal access (art. 360) and computer fraud (art. 249) require an organized criminal group to fall under the jurisdiction of DIICOT; in the absence of these conditions, jurisdiction falls to the prosecutor's offices attached to the courts/tribunals.

F. Banking financial crime in a cyber context

F.1. Money Laundering in a Cyber Context [xlii]

1. **Money laundering offence** (art. 49) of Law 129/2019: a) the exchange or transfer of goods, knowing that they come from the commission of offences, for the purpose of concealing or disguising the illicit origin of these goods or for the purpose of a person who takes care to try to commit offences. punishment; b) the concealment or disguising of the true nature, provenance, situation, disposition, circulation or ownership of goods or rights over them, knowing that the goods come from the commission of offences; c) c) the acquisition, possession or use of goods by persons other than the active subject of the offences from which the goods come, knowing that they come from the commission of offences. The attempt is punishable.

2. The financial intelligence unit of Romania is the National Office for the Prevention and Combating of Money Laundering (ONPCSB) (art. 1 para. 2)

- The competent authority that coordinates the assessment of the risks of money laundering and terrorist financing at national level, an assessment that is carried out within a cooperation mechanism with the authorities and institutions referred to in paragraph (1), as well as with self-regulatory bodies, ensuring the protection of personal data and professional secrecy under the terms of the law [xliii]. The Office is the competent authority that coordinates the national response to the assessed risks, including the working procedure and operational activity within the cooperation mechanism, and informs the European Commission, the European Banking Authority and the Member States in this regard. It receives notifications from obliged persons (banks, exchange offices, lawyers, notaries, accountants, bookmakers, real estate operators)
- When it finds indications of money laundering or terrorist financing, it informs **the Prosecutor's Office attached to the HIGH COURT OF CASSATION AND JUSTICE**

3. Reporting obligations (art. 5-7): **Immediate notification** to ONPCSB when there are suspicions that the operation is aimed at money laundering or terrorist financing; **Reporting of cash transactions** : within 10 working days for transactions ≥ **10,000 EUR** equivalent (lei or value) .

4. Relevance to cybercrime

- **Cryptocurrencies** and money laundering: high risks due to relative anonymity, insufficient regulation
- **The 2023 National Risk Assessment Report** identifies as a risk : "Purchasing cryptocurrencies with money obtained from criminal activities."
- **Cyber fraud (phishing, ransomware**) → money laundering through cryptocurrencies, international transfers, electronic payments[xliv]

5. Connection with cybercrime

Money laundering falls within the competence of DIICOT only if the money/property comes from the commission of crimes within the competence of DIICOT (therefore including

serious computer crimes within the competence of DIICOT) [Art. 11 para. (1) point 3 GEO 78/2016].

F.2. Relevant case law

A. Using bank cards

Decisions to unify the jurisprudence [xlv]of the High Court of Cassation and Justice :

Decision on mounting the device at ATMs and using cards:

1. **Installing skimmers , video cameras, fake keyboards at ATMs** according to art. 365 CP - illegal operations with computer devices)
2. **Using a genuine bank card without the holder's consent** for cash withdrawals = art. 250 para. (1) of the Criminal Code (performing fraudulent financial transactions)
3. **Using a counterfeit bank card** for withdrawals = art. 250 para. (1) of the Criminal Code + art. 313 of the Criminal Code (forgery of payment instruments) – actual concurrent offenses

Decision No. 53/2022 (HIGH COURT OF CASSATION AND JUSTICE) [xlvi]: **Unauthorized use of a bank card in contactless mode** at the POS terminal for product selection = art. 360 CP (illegal access to computer system) + art. 250 CP (fraudulent financial operations) – agreement

B. Other relevant decisions

Decision no. 37/2021 (HIGH COURT OF CASSATION AND JUSTICE) [xlvii]: Publishing fictitious products online that cause damage, without intervention in the computer system = **does NOT constitute a computer crime** , but fraud (art. 244 CP)

Decision no. 68/2021 (HIGH COURT OF CASSATION AND JUSTICE) [xlviii]: Analysis of the material element of the crimes of illegal access to an information system (art. 360 CP): the access operation must achieve intrusion/penetration into the system

Decision No. 15/2013 (HIGH COURT OF CASSATION AND JUSTICE) [xlix]: Discussion on the notions of "access" within the meaning of art. 360 of the Criminal Code; the need to clearly define access to avoid the extensive application of criminalization

G. Synopsis Table – Cybercrime Legislation Romania

Categories	**Regulatory act**	**Regulatory object**	**condition**	**Main sanctions**
Criminal charges	Criminal Code art. 249-252, 325, 360-366, 374	Cybercrime, fraud, child pornography	**Force**	3 months - 7 years in prison
Ratification of conventions	Law 64/2004	Budapest Convention (2001)	**Force**	International obligations
avert	Law 161/2003, Title III	Definitions, prevention measures, cooperation	**Partially in force** (art. 42-51 repealed)	Fine 5,000-50,000 lei (misdemeanor)
Cybersecurity	Law 58/2023	SNSC, COSC, competence, PNRISC, SNAC	**Vigor** (2023)	Fine 5,000-50,000 lei; up to 3% CA
NIS Directive	Law 362/2018	Essential service operators, digital service providers	**Vigor** (2018)	Cf. Law 58/2023

DNSC	Government Emergency Ordinance 104/2021	Establishment of DNSC, takeover of CERT-RO	**Vigor** (2021)	-
5G infrastructure	Law 163/2021	5G technology authorization, supply chain risk	**Vigor** (2021)	Offences, prohibitions on use
GDPR	EU Regulation 679/2016	Personal data protection	**Direct applicability** (2018)	Up to EUR 20 million or 4% of turnover
National GDPR	Law 190/2018	Apply GDPR Romania	**Vigor** (2018)	See GDPR
SPAM	Law 506/2004, art. 12	Unsolicited commercial communications	**Vigor** (2004)	Fine 5,000-100,000 lei; up to 2% of turnover
DIOCT	Government Emergency Ordinance 78/2016	Competence in organized crime, including cybercrime	**Vigor** (2016)	-
Money laundering	Law 656/2002	Preventing money laundering, including crypto	**Republic 2012**	Penalties CP
NIS2	EU Directive 2022/2555	Network and systems security (18 sectors)	**NOT TRANSPOSED** (deadline: Oct. 2024)	Anticipated: 4% of turnover or EUR 20 million

4. Areas of applicability of the law for computer crimes

Criminal acts depend on the nature of the crime. There is no international consensus on cybercrime. *The "Convention"* does not explicitly define the crime of "cybercrime". Cybercrime is used as a generic term for a wide range of activities carried out online and aimed at committing crimes.

In practice, it is found that there are **cybercrimes** in which we find traditional criminal activity that takes place "online" and does not require the use of a computer. Examples include: identity theft; fraud and incitement to violence; trafficking in prohibited substances; drug trafficking; coordination of terrorist activities, etc.

Also from practice we find that there are **cyber-dependent crimes** committed only through the use of information and communication technology devices. Examples include: spreading malware, encrypting databases and demanding substantial sums of money to unlock the owner's access to their own database.

Social engineering cybercrime . **Social** engineering cybercrime is a new phenomenon in society. In information security [l], social engineering means manipulating people to reveal sensitive data (passwords, codes, bank details) or provide access to systems and resources. Social engineering [li]is a form of psychological manipulation by which a person or group is determined to disclose confidential information or take actions that affect their safety, usually in the context of computer security and online fraud. It is based on exploiting the victim's trust, inattention or emotions (fear, urgency, curiosity, greed) to make them "cooperate". It is a first step for a complex fraud scheme and manifests itself [lii]through phishing messages:

emails/SMS/messages on social networks that imitate the bank, courier company, ANAF, etc. and ask for personal data or click on a malicious link.

The tactical field of social engineering is defined by the science of sociology applied in the digital environment with the express purpose of creating criminal situations and is carried out through a mix in which the criminal acts in the online space on the victim (from other state jurisdictions) and determines them to do certain actions that this finality victim is not aware of. Every person who provides the social media program, or the electronic mail address can become the victim of a cybercrime. The "Convention" considers that **international cooperation is necessary in a unified manner** and each state must adapt its domestic legislation and procedures to criminalize the following acts:

- damage, deletion, alteration or suppression of electronic data, when committed intentionally and without right;
- seriously hindering the functioning of an information and communications technology system by entering, transmitting, damaging, deleting, damaging, modifying or suppressing electronic data;
- misuse devices including programs designed or adapted primarily for the purpose of committing any of the computer crimes through Illegal access to the computer system, illegal interception, interference with electronic data or with an information technology system.
- The acquisition, production, sale, placing for use, import, distribution, making available or in any other way these devices constitute a crime only if they are used in criminal proceedings.
- The transmission of passwords, access data, electronic signatures or similar data through which the entire system or part of it can be accessed is classified as a crime;

States Parties shall consider and adopt such legislative and other measures as may be necessary to establish as criminal offences under domestic law the following acts committed intentionally and without right:

(a) Producing, offering, selling, distributing, transmitting, broadcasting, displaying, publishing or otherwise making available materials depicting child sexual abuse or sexual exploitation through an information and communications technology system;

(b) Solicit, procure or access materials depicting child sexual abuse or sexual exploitation of children through an information and communications technology system;

(c) Possession or control of child sexual abuse or sexual exploitation material stored on an information and communications technology system or other storage medium;

(d) Financing of stability offences in accordance with subparagraphs (a)-(c) of this paragraph, which States Parties may establish as a separate offence.

For the purposes of the Convention, the term *"material depicting sexual abuse or sexual exploitation of children"* includes visual material and may include written or audio content that depicts, describes any individual under the age of 18: (a) Engaging in real or simulated sexual activity; (b) In the presence of a person performing any sexual activity; (c) Sexual parts are displayed for primarily sexual purposes; or (d) Subjected to torture or cruel, inhuman or degrading treatment or punishment, and such material is of a sexual nature.

Conclusions and Recommendations

Conclusions and Recommendations on International Cooperation and National Resilience Against Cybercrime

The complex analysis of international cooperation mechanisms in the context of the adoption of the 2024 UN Convention, corroborated with the assessment of the legislative framework in Romania, leads to a series of fundamental conclusions.

The transition of judicial procedures from an approach based on strict territorial sovereignty to a collaborative, international digital governance, necessary to counter criminal phenomena in the " Dark Web" and the actions of hostile state actors, is evident.

The Jurisdictional Paradigm Shift: From Territoriality to Virtual Fluidity

The research confirms that the classic principle of geographical territoriality has become insufficient in combating cybercrime.

- ✓ **Decoupling Crime from Location:** Adoption of the United Nations Convention (2024) formal recognition that criminal jurisdiction must follow the flow of data, not physical borders. Complementarity between state authorities is mandatory, not optional, given that digital evidence is volatile and a state's critical infrastructure can be attacked from servers located " offshore " or unstable.
- ✓ **Global Standardization vs. National Specificity:** Although the Convention respects sovereignty (Art. 5), its effectiveness depends on the ability of states to harmonize definitions of crimes (such as illegal access or interception of data) to facilitate letters rogatory and the rapid preservation of electronic evidence.

Maturity and Stratification of the Legislative Framework in Romania

The analysis of national legislation demonstrates that Romania has overcome the reactive adaptation phase, having a layered and robust legislative system, although there are implementation vulnerabilities.

Strengthening Criminalization (Criminal Code): The integration of cybercrimes into Title VII of the Criminal Code and the constant updating of penalties (e.g. Art. 360-365) show a maturation of criminal policy. Romania has clear instruments to sanction all crimes against system security, as well as computer fraud (Art. 249 CP), covering the spectrum from " hacktivism " to organized financial crime.

The State's Institutional Architecture for Cybersecurity: The establishment of the National Cybersecurity Directorate (DNSC) and the functioning of the Cybersecurity Operational Council (COSC) under the aegis of the CSAT places cybersecurity directly at the center of national security. Law 58/2023 provides the necessary levers for a rapid response, transforming cybersecurity from a technical issue into one of national defense.

Critical Vulnerabilities and Emerging Challenges

In the legislative context, the research material identifies critical points that require immediate attention:

- ➢ **Lack of NIS2 Transposition into National Law:** The delay in transposing the NIS2 Directive (status December 2025) creates a systemic vulnerability. The extension of essential sectors (from energy to waste management) and a more drastic sanctioning regime are vital to

respond to the private and public sector. The absence of this framework leaves operators of essential services exposed to heterogeneous security standards.

➢ **The Challenge of the " Dark Web" and Cryptocurrencies :** The material highlights a worrying trend in the area of crypto reserves (e.g. the models of El Salvador, USA, China). Cybercrime is no longer just the prerogative of independent hackers, but is becoming a source of financing for regimes or paramilitary organizations. The capacity of the Romanian state to identify, seize and capitalize on crypto assets (extended confiscation) must keep pace with the innovation of criminals who use currency mixers and decentralized services.

The Balance Between Security and Fundamental Rights

A major conclusion of the research concerns the ongoing tension between investigation efficiency and privacy protection. **Surveillance vs. GDPR:** The international cooperation and data retention mechanisms of the UN Convention and national legislation (Law 161/2003, Law 506/2004) must be applied with extreme rigor in order not to violate the GDPR Regulation. The risk that cyber investigations become excessively invasive is real, and **procedural guarantees must remain an active filter, not just theoretical** .

Based on the research, the following directions of action are required:

1. **Urgent NIS2 Transposition:** Immediate alignment of European NIS2 standards to avoid infringement procedures and, more importantly, to secure the digital supply chain.
2. **Specialization of Magistrates:** Continuing the training of prosecutors and judges not only in criminal law, but also in understanding technical phenomena from the area of cybersecurity and cybercrime (blockchain, AI, DDoS attacks), considering the complexity of the cases described (Art. 250 CP vs Art. 365 CP).
3. **Cyber Diplomacy:** Romania must play an active role in the operationalization of the UN Convention, using its expertise (the Cyber hub in Bucharest) to facilitate cooperation between the EU and those outside the community space.

In conclusion , cybersecurity is no longer an option, but a condition for the existence of the modern state. The United Nations Convention on Cybercrime, from 2024, provides the global framework, but real resilience depends on Romania's ability to adapt and rigorously apply domestic legislation but also on anticipation of technological mutations of organized cybercrime.

REFERENCES

[i] https://ro.wikipedia.org/wiki/Dark_web

[ii] https://intelligence.sri.ro/dark-web-agora-criminalitatii-cibernetice/

[iii]Baranenko, Roman. (2021). Cybercrime, computer crime or cybercrime? Analysis of the characteristics of a terminological application. Journal of the National Technical University of Ukraine. Political Science. Sociology. Law. 85-90. 10.20535/2308-5053.2021.1(49).233023.

[iv] https://www.juridice.ro/771491/tehnologia-in-campaniile-electorale.html

[v] *Enterprise Data Strategy – Empowering Data-Informed Diplomacy, September 2021* , Department of State, United States of America, https://www.state.gov/wp-content/uploads/2021/09/Reference-EDS-Accessible.pdf

[vi] *On the Ladder from Ransomware to Cyberterrorism: The Cases of JBS USA, Colonial Pipeline, and Wiperware Attacks Against Ukraine* , Journal of Cyber Policy, 2024.

[vii] Isaac, Reji. (2011). Application of cybernetics in cybercriminology. 10.13140/RG.2.1.4263.6565.

[viii] https://doi.org/10.1080/14751798.2024.2321736

[ix] https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime Accessed on 28.12.2025

[x]Council Decision (EU) 2025/2307 of 13 October 2025 on the signing, on behalf of the European Union, of the United Nations Convention against Cybercrime; (OJ L, 2025/2307, 11.11.2025, ELI: http://data.europa.eu/eli/dec/2025/2307/oj).

[xi] https://data.consilium.europa.eu/doc/document/ST-14941-2025-INIT/ro/pdf (page 6)

[xii] https://zic.legal/infractiuni-informatice-in-romania/

[xiii] https://tapu.ro/ro/infractiunile-informatice-ce-spune-legea-despre-hacking-phishing-sau-frauda-online/

[xiv]Law 161/2003 on some measures to ensure transparency in the exercise of public dignities, public functions and in the business environment, the prevention and sanctioning of corruption, Official Gazette no. 279 of 2003, with subsequent amendments and supplements.

[xv] https://www.sri.ro/cyberint

[xvi]Decision 1321/2021 on the approval of *the Cybersecurity Strategy of Romania, for the period 2022-2027, as well as the Action Plan for the implementation of the Cybersecurity Strategy of Romania, for the period 2022-2027* , Official Gazette no. 2 of 2022.

[xvii] https://www.dnsc.ro/

[xviii] https://www.ancom.ro/

[xix] https://www.mai.gov.ro/

[xx] https://www.sri.ro/

[xxi] https://www.mapn.ro/

[xxii] https://sie.ro/

[xxiii] https://sts.ro/ro/

[xxiv] https://www.spp.ro/#/

[xxv] https://orniss.ro/

[xxvi] https://pnrisc.dnsc.ro/

[xxvii]Criminal Code (Law 286/2009) – art. 249-252, 325, 360-366, 374

[xxviii]https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf

[xxix]Law 362/2018 on ensuring a high common level of security of networks and information systems, Official Gazette no. 21 of 2019, with subsequent amendments and supplements.

[xxx]Emergency Ordinance 104/2021 on the establishment of the National Cyber Security Directorate, Official Gazette no. 918 of 2021, with subsequent amendments and supplements.

[xxxi]https://www.universuljuridic.ro/oug-nr-104-2021-privind-infiintarea-directoratului-national-de-securitate-cybernetica-contraventii-si-sanciuni/

[xxxii]Law 163/2021 on the adoption of measures regarding the information and communications infrastructure of national interest and the conditions for the implementation of 5G networks, Official Gazette no. 590 of 2021, with subsequent amendments and supplements.

[xxxiii]Law 163/2021 on the adoption of measures regarding the information and communications infrastructure of national interest and the conditions for the implementation of 5G networks, Official Gazette no. 590 of 2021, with subsequent amendments and supplements.

[xxxiv]Law 163/2021 on the adoption of measures regarding the information and communications infrastructure of national interest and the conditions for the implementation of 5G networks, Official Gazette no. 590 of 2021, with subsequent amendments and supplements.

[xxxv] https://www.mae.ro/node/28367#null

[xxxvi] https://www.certsign.ro/ro/directiva-nis2-trei-masuri-pentru-o-securitate-cybernetica-conforma/

[xxxvii]Law 190/2018 on implementing measures for Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on *the protection of natural persons with regard to the processing of personal data and on the free movement of such data* , and repealing

Directive 95/46/EC (Official Regulation No. protection), General Data Protection Monitor. 651 of 2018, as subsequently amended and supplemented.

[xxxviii] https://www.dataprotection.ro/

[xxxix]Law 190/2018 on implementing measures for Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Official Regulation No. protection), General Data Protection Monitor. 651 of 2018, as subsequently amended and supplemented.

[xl]Law 506/2004 on the processing of personal data and protection of privacy in the electronic communications sector, Official Gazette no. 1101 of 2004, as subsequently amended and supplemented.

[xli] https://www.diicot.ro/prezentare/legislație

[xlii]Law 129/2019 on the prevention and combating of money laundering and terrorist financing, as well as on the amendment and completion of certain normative acts, Official Gazette no. 589 of 2019, with subsequent amendments and completions.

[xliii]Law 129/2019 on the prevention and combating of money laundering and terrorist financing, as well as on the amendment and completion of certain normative acts, Official Gazette no. 589 of 2019, with subsequent amendments and completions.

[xliv] https://blog.cursuribursa.ro/care-sunt-cele-mai-frecvente-scheme-de-spalarea-banilor/

[xlv]Law 506/2004 on the processing of personal data and protection of privacy in the electronic communications sector, Official Gazette no. 1101 of 2004, as subsequently amended and supplemented.

[xlvi] https://www.iccj.ro/2022/11/22/decizia-nr-53-din-28-septembrie-2022/

[xlvii] https://www.iccj.ro/2021/07/19/decizia-nr-37-din-7-iunie-2021/

[xlviii] https://www.iccj.ro/2022/01/20/decizia-nr-68-din-29-septembrie-2021/

[xlix] https://www.iccj.ro/2013/10/14/decizia-nr-15-din-14-octombrie-2013/

[l] https://help.eset.com/glossary/ro-RO/social_engineering.html

[li] https://ro.wikipedia.org/wiki/Social_engineering

[lii] https://ro.safetydetectives.com/blog/what-is-social-engineering/