The Fight Against Terrorism in the Digital Era: Policing Perspectives, Legislative References, and Cybercrime Dimensions

Ștefan-Gabriel DASCĂLU, Marius-Andrei OROȘANU
Police Academy “A.I. Cuza” Bucharest, Romania
stefan.dascalu@academiadepolitie.ro, andrei.orosanu@academiadepolitie.ro

Abstract

The digital era has transformed both the nature of terrorism and the mechanisms designed to combat it. Contemporary terrorist organizations increasingly exploit cyberspace for recruitment, propaganda, financing, and operational coordination, thus blurring the boundaries between physical and virtual threats. This paper examines the evolving role of law enforcement agencies in addressing these challenges, emphasizing the need for advanced technological tools, interagency cooperation, and continuous adaptation of policing strategies. Furthermore, it analyzes the legislative frameworks that underpin counterterrorism policies within the digital domain, highlighting existing gaps and the growing intersection with cybercrime. By integrating legal, operational, and technological perspectives, the study aims to provide a comprehensive understanding of how digitalization reshapes both terrorism and the institutional responses designed to counter it.

Index terms: counterterrorism, cybercrime, digital foreign policy, European Union, law enforcement cooperation

1. Introduction

Terrorism represents one of the most serious threats to international security, public order, and the democratic values of the contemporary world. From large-scale attacks such as those of September 11, 2001, to targeted assaults carried out in European capitals - Paris, Brussels, London, Madrid - the terrorist phenomenon has continuously adapted, diversifying its methods, targets, and operational means. Today, terrorist organizations exploit technology, online radicalization, failed-state environments, organized crime networks, and global mobility, which confer upon the phenomenon a fluid, unpredictable nature that is increasingly difficult to counter through traditional means [1].

Transformations in the security environment have compelled states to reorient toward a modern policing model grounded in prevention, intelligence, integrated action, and international cooperation. Whereas traditional terrorist structures once operated hierarchically with visible leaders, command centers, and clear chains of command current trends reveal a shift toward fragmented entities: autonomous cells, “lone wolves,” multi-nodal networks, and hybrid groups with ideological, criminal, and paramilitary dimensions. This evolution obliges institutions responsible for counterterrorism to develop proactive capabilities, adopt flexible investigative methods, and rapidly exploit operational intelligence [2].

Across Europe, the rise in high-impact attacks such as the Bataclan (2015) and Brussels (2016) incidents has prompted the revision of counterterrorism strategies and strengthened police cooperation within the European Union. The United Nations has also enshrined, through its resolutions, the obligation of states to adopt legislative, administrative, and operational measures for the prevention and suppression of terrorism. The European Union has transposed these standards through legal instruments, operational mechanisms, and specialized structures, while Romania has aligned its domestic framework, institutional responsibilities, and investigative techniques with current risks [3].

At the national level, counterterrorism efforts are closely linked to broader initiatives aimed at preventing and combating organized crime, given the increasingly evident intersection between the two phenomena particularly in areas such as financing, arms trafficking, use of forged documents, and logistical support. Terrorism-related investigations require a high degree of interinstitutional cooperation, operational coordination, and procedural standards compatible with those of the European Union.

In this context, the present study aims to:

- Highlight the essential legislative landmarks (UN, EU, Romania).
- Analyze the dynamics of the terrorist phenomenon and its implications for policing activities.
- Present modern operational directions, including elements of prevention, early detection, intervention, investigation, and international cooperation.

The article approaches terrorism from a policing perspective, emphasizing an integrated operational cycle prevention, counteraction, and investigation as well as the need to optimize both punitive and non-punitive instruments while safeguarding fundamental rights. Through this structure, the research combines legal analysis with contemporary operational methodologies, offering a realistic and applied perspective on counterterrorism.

2. Legal Frameworks in Counterterrorism

The fight against terrorism is grounded in a comprehensive set of legal instruments operating across three levels: global (United Nations), regional (European Union), and national (Romania). These instruments establish state obligations, minimum action standards, and key principles governing police cooperation, information exchange, prevention of radicalization, and the conduct of specific operational activities.

2.1. United Nations Level - Global Standards

The United Nations has gradually developed a universal legal framework founded on the obligation of states to prevent, investigate, and punish terrorist acts. The core documents include:

UN Security Council Resolution 1373 (2001), adopted in the aftermath of the September 11 attacks, which requires states to: criminalize terrorist-related acts; freeze terrorist funds and financial resources; strengthen international cooperation (extradition, mutual legal assistance, data exchange); reinforce border control mechanisms.

The United Nations Global Counter-Terrorism Strategy (2006, revised 2010-2016), which introduced a proactive and police-preventive approach, emphasizing cooperation among national agencies, measures against radicalization, and the reduction of factors conducive to terrorism.

A series of UN sectoral conventions, addressing aircraft hijacking, protection of diplomats, terrorist financing, and bomb attacks, among others, which oblige states to criminalize such acts and cooperate internationally.

Key UN principle: Terrorism is a global threat that requires a coordinated response focused on prevention, cooperation, and disruption of financing channels [4].

2.2. European Union Level - Common Security and Police Cooperation

The European Union has developed one of the most advanced regional systems for combating terrorism, combining criminal legislation with operational mechanisms and intelligence-based instruments.

Key documents and mechanisms:

The EU Counter-Terrorism Strategy (Council of the EU, 2005), structured around four pillars: *Prevent - Protect - Pursue - Respond*.

Directive (EU) 2017/541 on Combating Terrorism, which obliges Member States to criminalize:

- preparation and facilitation of terrorist acts.
- recruitment and training for terrorism.
- travel for terrorist purposes ("foreign fighters").
- terrorist financing.

Operational instruments:

- *Europol* - European Counter Terrorism Centre (ECTC).
- *Eurojust* - judicial coordination.
- *SIS II*, *PNR*, and *Prüm* systems - data exchange for suspect identification.
- *Frontex* - border management and detection of terrorist routes.

The EU model is operational in nature, emphasizing real-time police and intelligence cooperation within a common security framework.

2.3. Romania's Level - National Legislative and Institutional Framework

Romania has aligned its legislative and operational systems with UN and EU standards.

Core elements:

Law No. 535/2004 on the Prevention and Combating of Terrorism, the main legislative act, which:

- defines terrorism and related offenses.
- establishes the *National System for Preventing and Combating Terrorism (SNPCT)*.
- designates the Romanian Intelligence Service (SRI) as the national authority in this field.
- regulates interinstitutional cooperation and operational measures.

Key institutions:

- *SRI* - coordination of SNPCT and intelligence component.
- *Ministry of Internal Affairs (MAI)* - Romanian Police, Gendarmerie, SIAS units, and other operational structures.
- *DIICOT* - criminal prosecution in terrorism-related cases.
- *MAE, MApN, SPP, STS* - specialized institutional support.

Complementary legislation:

- The *Criminal Code* and *Criminal Procedure Code* (special investigative measures).
- The *Law on the Prevention and Combating of Terrorist Financing*.
- Regulations on border control, population records, and identity documents.

Characteristic of the Romanian system: a hybrid model combining a strong intelligence component (SRI) with an operational policing one (MAI + DIICOT).

The three levels UN, EU, and Romania together constitute a coherent legislative framework. However, actual effectiveness depends on the operational dimension, which will be examined in subsequent chapters: prevention, investigation, cooperation, operational analysis, and the application of modern counterterrorism tools [5].

3. The Dynamics of the Terrorist Phenomenon and the Operational Dimension in the Digital Environment

For practitioners, terrorism is not an abstract category but a process with distinct phases - recruitment, financing, training, mobilization, execution, consolidation/propaganda - and each phase requires specific detection and intervention tools and methods. This section outlines the dynamic elements that must be monitored at the operational level.

Contemporary terrorism can no longer be understood outside the virtual space. Whereas in the past terrorist organizations relied primarily on physical contacts, clandestine networks and traditional logistical circuits, the digital environment now provides a complete ecosystem for recruitment, propaganda, financing, encrypted communication, procurement, operational planning and training. Cyberspace thus becomes the force multiplier of modern terrorism, and the interaction between terrorism and cybercrime produces a hybrid threat with unprecedented dynamics.

3.1. General Considerations from a Policing Perspective

A policing approach to counterterrorism requires the integration of the normative framework with proactive operational mechanisms oriented toward prevention, monitoring, deterrence and the neutralization of radicalized groups or individuals. In the current security climate marked by intensified online radicalization, increased cross-border mobility and ready access to highly lethal means of attack police authorities must adopt flexible, integrated methods founded on real-time information sharing.

In Romania, operational responsibilities are distributed among specialised structures of the Ministry of Internal Affairs (MAI), the Romanian Intelligence Service (SRI), the Public Prosecutor's Office and European cooperation bodies. Specifically, the police play a central role in: early identification of risk indicators, collection and exploitation of operational information, documentation of offences, executing procedural actions and supporting anti-terrorist intervention units during the critical phase of a threat. This approach reflects current counterterrorism principles, whereby prevention remains the primary strategic objective and the use of force is a last resort, applicable only when all preventive mechanisms have failed.

Police investigations into terrorist modus operandi focus on the operational chain: radicalization → financing → recruitment → planning → logistic preparation → execution → claim of responsibility → propaganda and regeneration. Each link in this chain represents an opportunity for intervention and disruption, which explains why modern strategies emphasize early detection of intent and discreet surveillance of high-risk environments (unauthorised places of worship, clubs, prisons, encrypted forums, social networks, etc.).

Consequently, the policing perspective is characterised by several defining features:

- orientation toward prevention and anticipation.
- action based on operational intelligence rather than merely post-factum reaction.
- a multi-institutional approach.
- continuous surveillance of risk environments and cross-border flows.
- rapid and lawful intervention during the early stages of attack preparation.

This operational logic is consistently reflected in European practice, and the attacks in Paris (Bataclan, 2015) and Brussels (2016) demonstrated that the window between radicalization and action can compress dramatically, sometimes to only a few days, thereby imposing accelerated investigations and efficient police-cooperation mechanisms.

3.2. The Role of Operational Structures and Inter-Institutional Cooperation

Countering terrorism requires a complex institutional architecture in which policing structures operate in an integrated manner with intelligence services, specialised public prosecutors' offices and international organisations. From the perspective of operational investigation, the police have two fundamental missions: the acquisition of information and the disruption of a potential perpetrator's operational capacity. This role can be fulfilled only within a cooperative framework in which data exchange, integrated analysis and the synchronization of interventions are functional.

Nationally, cooperation is principally effected through coordination structures and joint operational centres representing the Ministry of Internal Affairs, competent prosecution offices and the Romanian Intelligence Service. The dynamics of the phenomenon oblige institutions to communicate in real time, because the operational window for preventing an attack is narrow and any bureaucratic bottleneck can transform a mere operational signal into a tragedy. The Bataclan explosion in 2015 and the Brussels attacks in 2016 demonstrated at the European level that the absence of rapid information exchange among law-enforcement bodies can allow terrorist cells to travel, finance themselves and equip without detection.

At the international level, police forces use an extensive cooperative toolkit that includes:

- *Europol* (EC3, ECTC) - operational analysis, support in investigating networks, cross-border forensic intelligence.
- *Interpol* - databases on wanted persons, forged documents, weapons and foreign terrorist fighters (FTF).
- *SIRENE & SIS II* - real-time alert flows for suspects and fraudulently used documents.
- *Frontex* - a critical actor in mobility and border control for filtering risks.

Such cooperation enables national police to see beyond their borders, which is essential since contemporary terrorism does not respect territorial limits.

3.3. Radicalization, Propaganda, Financing and Recruitment in the Online Environment

Social platforms, forums and encrypted messaging applications have become the principal instruments through which terrorist networks:

- disseminate highly emotive visual and narrative propaganda.
- recruit vulnerable youth within the EU.
- create ideological bubbles that are difficult for authorities to penetrate.
- organize micro-digital communities that later translate into offline action.

ISIS, Al-Qaeda and their affiliates have developed sophisticated media factories, exploiting Twitter, Telegram, TikTok, Discord and the digital diaspora. Radicalization is no longer centralized but individualized and automated, assisted by platform algorithms that promote extremist content to susceptible users.

The Dark Web - the hidden infrastructure of digital terrorism

The Dark Web functions as a global marketplace for illegal goods and services, including:

- weapons and components for improvised explosive devices (IEDs).
- personal data, bank accounts and stolen identities.
- hacking services, ransomware or DDoS capabilities.
- false passports and transit documents.
- manuals on explosive-making, urban tactics and counter-surveillance techniques.

This parallel space allows terrorists to purchase goods, communicate and obscure their traces thanks to:

- TOR / I2P networks.
- PGP encryption.
- escrow platforms.
- bulletproof servers hosted in hostile jurisdictions.

Cryptocurrency financing of terrorism has, in recent years, moved beyond isolated experiments to become a relevant component of the digital underground economy associated with jihadist organisations and other extremist groups. Terrorists have adopted virtual currencies as a funding instrument that is difficult to trace:

- Bitcoin, Monero, Zcash.
- anonymised electronic wallets.
- mixers/tumblers for laundering funds.
- covert fundraising through sham NGOs or crypto-charity campaigns.

Operational Advantages for Terrorist Networks

Advantage (English)	Explanation
Relative anonymity	Conceals the true identity of the ultimate beneficiary.
Cross-border nature	Operates beyond the scope of conventional banking controls.
Speed	Transfers can be executed within minutes.
Convertibility to cash	Can be exchanged for cash via cryptocurrency ATMs or informal exchangers.

These mechanisms complement traditional funding sources (trafficking, fraud, donations) rather than replacing them, rendering the phenomenon more resilient and less conspicuous.

According to Europol and the Financial Action Task Force (FATF), the current trend is no longer the concentration of large sums in a single transaction but the fragmentation into micro-flows below the detection thresholds of banking systems - a method perfectly compatible with autonomous terrorist cells and low-cost attacks.

Encrypted Communication and Cooperation between Terrorists and Hackers

Terrorist actors employ end-to-end encryption (e.g., Telegram, Signal, ProtonMail) to evade interception. Increasing evidence indicates that certain terrorist groups:

- collaborate with financially motivated hackers (crimeware-as-a-service).
- purchase exploits and malware.
- commission cyberattacks against critical infrastructure.

Thus, the relationship between terrorism and cybercrime is evolving from a mere connection into a complementary pact.

3.4. The Operational Cycle of Counterterrorism Investigation

Counterterrorism investigations follow a specific cycle distinct from classical criminal inquiries, as their main objective is not to prove the offence after it has occurred, but to interrupt the operational chain before the lethal outcome materializes. In both doctrine and practice, the police counterterrorism cycle includes:

- Identification of early warning signals - monitoring high-risk environments, online surveillance, behavioural analysis, and assessment of interactions with potential radical structures.
- Collection and verification of information - HUMINT, SIGINT, OSINT, technical surveillance, and undercover investigations.
- Assessment of threat level and target prioritization - according to intent, capability, and proximity to action.
- Documentation and evidentiary consolidation - as far as possible without compromising intelligence operations.
- Neutralization through coercive measures - arrest, searches, logistical disruption, and freezing of financial flows.
- Post-intervention intelligence exploitation - aimed at preventing cell regeneration.

This cycle implies that, operationally, the police act with one hand in the intelligence domain and the other in the criminal justice sphere, in finely tuned synchronization with intelligence services and specialized prosecutors' offices.

3.5. Operational Prevention and Counter-Radicalization

Prevention constitutes the first line of defence in counterterrorism, grounded in the concept of *"intervention before intent"* - identifying radicalization processes early and disrupting them before they evolve into violent action.

From a policing standpoint, prevention has two complementary dimensions:

- Operational (hard) prevention - surveillance of individuals and environments with terrorist potential, monitoring vulnerable areas, gathering intelligence, and conducting deterrence actions.
- Community and social (soft) prevention - local partnerships with relevant social actors (schools, families, religious institutions, NGOs, and local authorities).

The radicalization process is gradual and long-term, fueled by socio-economic frustrations, ideological narratives, and digital influences.

Operationally, the police have a duty to understand high-risk environments, engage with them, and intervene proactively through:

- identification and limitation of the influence of radical "preachers".
- monitoring of spaces where violent propaganda circulates.
- collaboration with community leaders and social services.
- early notification of intelligence agencies when clear signs of radicalization emerge.

The online environment currently represents the most dynamic arena for radicalization, as it offers anonymity, access to extremist materials, direct contact with recruiters, and the creation of "ideological bubbles."

Consequently, modern prevention cannot exist without a strong *cyber-police* and *cyber-intelligence* component.

3.6. Combating the Financing of Terrorism - A Policing Perspective

Financing represents the *"oxygen of terrorist organizations."* Even small cells operating under a low-cost model as seen in numerous European attacks between 2015 and 2018 require funding for:

- logistical expenses (safe-house rent, transport, communication).
- procurement of weapons or chemical precursors.
- forgeries, documentation, and operational support.

The role of the police is to asphyxiate financial resources, using mechanisms that include:

- tracing banking flows through Financial Intelligence Units (FIUs).
- monitoring suspicious transactions, including micro-payments.
- cooperating with private financial institutions (banks, non-banking entities).
- tracking online funding through cryptocurrencies, crowdfunding, or disguised donations.
- applying extended confiscation and rapid precautionary measures before funds are dispersed.

European experience shows that contemporary jihadism relies on a hybrid mix of sources: personal savings, cyber fraud, trafficking, "charitable" donations, cryptocurrencies, and funding from state sponsors. Therefore, police authorities must treat the financial component as a mandatory parallel investigation, not as a secondary element [6].

3.7. Modern Operational Techniques in Countering Terrorism

The counterterrorism operational field has shifted into a hybrid zone in which police must combine classical methods with intelligence tools and technological expertise. The most commonly employed modern techniques are summarized below.

Category	**Operational Tools**
SURVEILLANCE	physical tailing, operational surveillance techniques, geolocation, drones in urban environments
OSINT	social-media monitoring, encrypted forums, Dark Web monitoring
SIGINT	interception, communications analysis, metadata analysis
Undercover HUMINT	infiltrators, collaborators, human sources within the diaspora or religious communities
Digital forensics	exploitation of phones, servers, cloud services, and crypto-wallets

Compared with organised-crime investigations, counterterrorism inquiries demand greater speed because the optimal intervention moment is prior to the execution phase; police must therefore apply a zero-tolerance approach to risk. This requires a high operational standard, including:

- parallel documentation of evidence for the Prosecutor’s Office.
- filtering of raw intelligence through analytical units.
- “hit-and-freeze” actions: entry - capture - neutralization.

All these techniques are reflected in national doctrine, which emphasizes early intervention, disruption of logistics, and separation of the perpetrator from their resources.

3.8. Tactical Intervention Management and the Neutralization of Terrorist Cells

Neutralizing a terrorist actor requires an integrated operational chain that combines the intelligence component with tactical action. Unlike organised crime - where intervention timing may be chosen strategically to document an entire network - in terrorism the priority is not necessarily total network dismantlement but the prevention of loss of life.

Modern police and counterterrorism procedures for tactical intervention are based on the following principles:

Intervention within the “short window” - act immediately once there are clear indications that an attack is imminent. Waiting is excluded, as it risks irreversible consequences.

- Segmentation of the operational area - rapidly separate suspects from civilians, isolate the perimeter, and control flows (evacuation, communications, transport).
- Neutralization with proportionate force - apply force progressively but with a clear mandate: the suspect must be neutralized before they can detonate, attack, or escape.
- Protection of evidence and the information chain - to ensure judicial finality, electronic, biological and documentary evidence must be preserved and processed immediately.
- Priority on “capture” rather than “elimination” when feasible - to enable intelligence exploitation, particularly regarding the logistics network (financing, recruitment, communications).

European experience (Belgium 2016, Germany 2018, France 2020) has shown that mixed teams (intervention - negotiation - technical exploitation - analysts) increase operational efficiency by over 50%, as they provide a multi-dimensional real-time response [7].

3.9. International Cooperation and Operative Information Exchange

Terrorism is transnational in terms of mobility, financing, communications and ideology; consequently, a purely national response is structurally insufficient. Modern policing operates within a cooperative architecture that includes:

- *Europol* (ECTC - European Counter-Terrorism Centre) - an analytical and operational hub for terrorist situations with real-time database access.

- *Interpol* - international notices and follow-ups, including those concerning Foreign Terrorist Fighters.
- *SIRENE* and *SIS II / SIS Recast* - immediate operational exchange within the EU.
- *PNR, API, FRONTEX* - for monitoring passenger and border flows.
- informal HUMINT networks obtained via internal-affairs attachés, liaison officers and Joint Investigation Teams (JITs).

A critical element in police counterterrorism work is the speed of data exchange. In the terrorism domain, "delayed" information is effectively useless. Therefore, the current European architecture is built on:

- exchange in minutes and hours, not days and weeks.
- direct access to shared databases without bureaucratic detours.
- interoperability of databases (SIS, VIS, Eurodac, PNR, ECRIS).

These mechanisms are particularly effective in identifying fighters returning from Syria-Iraq, mobile propagandists and cells traversing Schengen routes.

Countering terrorism from a policing perspective entails:

- early prevention through monitoring, social education and counter-radicalization.
- disruption of violent actors' logistical and financial resources.
- rapid tactical intervention aimed at saving lives.
- continuous investigation and intelligence exploitation even after the target has been neutralized.
- permanent international cooperation, in the logic of "zero gaps between systems."

If organised crime pursues profit, terrorism pursues impact; the only effective response is proactive, integrated and decisive policing, supported by law but not constrained by it operationally. In this equation, time becomes the primary operational currency: whoever acts first wins [8].

4. General Conclusions and Modern Directions in Counterterrorism Action

4.1. General Considerations

Contemporary terrorism is no longer an isolated manifestation but a complex form of organized violence encompassing political, ideological, religious, and technological dimensions. In the 21st century, it continuously reinvents itself, adapting to geopolitical shifts, technological vulnerabilities, and the social tensions of a globalized world.

From a policing perspective, the fight against terrorism extends far beyond identifying and neutralizing perpetrators. It involves the integrated management of the broader criminal ecosystem surrounding the phenomenon of radicalization, propaganda, financing, logistical support, recruitment, and the exploitation of the digital space.

Modern police forces should be regarded as *operational intelligence actors*, not merely reactive forces. They occupy the center of the preventive, investigative, and intervention mechanism, serving as the connective node between the legal, intelligence, and tactical domains within a unified framework of coordinated action.

4.2. Integrating the Legislative Dimension into the Policing Approach

The legal framework-national, European, and international-provides both the foundation of legality and the operational flexibility required by field structures. The UN counterterrorism conventions, the EU Framework Decisions and Directives, and Romanian legislation (Law No. 535/2004 on the Prevention and Combating of Terrorism, the Criminal Code, and the National Security Law) form a coherent system designed to:

- legally define the terrorist phenomenon.
- establish the competences of responsible institutions.

- regulate special investigative and intervention means.
- ensure sanctions proportionate to the gravity of the acts committed.

However, the effectiveness of these instruments depends not merely on their normative existence but on the *operational capacity and interinstitutional coordination* behind their implementation. Where the law provides the framework, the police must provide the action.

4.3. Modern Directions in Counterterrorism Action

Recent European and global developments reveal five key modern directions in counterterrorism, particularly relevant for police structures:

- Artificial Intelligence and Predictive Analysis - employing algorithms for detecting suspicious behavior, facial recognition, and correlating multi-source data flows (SIS, Europol, Interpol, OSINT).
- Countering Online Radicalization - monitoring extremist narratives, removing radical content, and developing counter-messaging through educational and civic platforms.
- Strengthening International Cooperation - enhancing database interoperability, creating regional analysis and intervention centers, and ensuring real-time sharing of operational intelligence.
- Adapting Urban Intervention Tactics - training police units for rapid response in crowded environments and neutralizing mobile targets while respecting the principle of proportionality.
- Combating Terrorist Financing and Logistical Support - reinforcing Financial Intelligence Units (FIUs), tracing cryptographic transactions, and cooperating with private-sector entities (banks, fintech, transport, communications).

These directions reflect the increasing integration of technology and behavioral analysis into police operations, marking the transition from *reactive policing* to *anticipatory policing*.

4.4. Recommendations for Policing Practice

Based on legislative, operational, and institutional analysis, the following recommendations can be formulated:

- Develop data-analysis capabilities (*big data policing*) and train personnel in OSINT and cyber-intelligence.
- Strengthen the culture of partnership among police, community, and the private sector.
- Implement unified response mechanisms (*joint task forces*) for terrorist-risk situations.
- Establish a National Counterterrorism Training Centre within the Ministry of Internal Affairs, modeled after Europol's ECTC.
- Intensify the exchange of best practices with EU member states and NATO partners in the fields of *tactical intelligence* and *counter-radicalization*.

4.5. Final Conclusions

Terrorism cannot be completely eradicated, but it can be controlled and prevented through anticipation, coordination, and decisive action.

The modern state must base its response on two complementary pillars: law and operational capability. Within this framework, the police is no longer merely an enforcer of the law, but a strategic actor of national and international security. Its capacity to collaborate, analyze, and respond swiftly represents the most effective deterrent against terrorism.

The prevailing consensus in the specialized literature is unequivocal: the next principal arena of terrorist financing will be the crypto-digital environment. Consequently, the fight can no longer rely solely on classical legal instruments but must incorporate cyber-investigation, transnational cooperation, and digital policing techniques.

References

[1]. Security Council of UN, 3 DECEMBER 2001, “Resolution 1373”, Available: https://legislatie.just.ro/Public/DetaliiDocument/32477.

[2]. Ștefan-Gabriel DASCĂLU, 2016 *“Combaterea criminalității organizate”* publisher: SITECH, city: Craiova, pp. 335-339.

[3]. United Nations, 2006, “Global Counter-Terrorism Strategy.” Available: https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy.

[4]. European Council, 2018, “UE Strategy for countering terrorism”, Available: https://eur-lex.europa.eu/TodayOJ/.

[5]. EUROPOL, 2016-2017 “Terrorism Situation and Trend Report”, Available: https://www.europol.europa.eu/publications-events/main-reports/tesat-report.

[6]. OSCE, 25 March 2019, “Preventing Terrorist Radicalization”, Available: https://www.osce.org/event/osce-wide-counter-terrorism-conference-2019.

[7]. Financial Action Task Force, 2022 “FATF Annual Report 2022-2023”, Available: https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2022-2023.html.

[8]. EUROPOL, 2022 “European Counter Terrorism Centre - ECTC operational report”, Available: https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc.