

Problems of criminalising cyberterrorist offences and their financing in Ukraine: Doctrinal analysis and proposals for legislative amendments

Vladyslav Kubalskyi^{1,†}, Pavlo Kasyanov^{2,3,†} and Maksym Kysil^{1,*,†}

¹V. M. Koretsky Institute of State and Law of the National Academy of Sciences of Ukraine, Triokhsviatytska Str., 4, Kyiv, 01001, Ukraine

²Institute for Applied System Analysis, Beresteiskii Ave., 37(35), Kyiv, 03056, Ukraine

³Kyiv School of Economics, Mykoly Shpaka Str., 3, Kyiv, 03113, Ukraine

Abstract

The article provides a comprehensive study of the criminal-law mechanisms for countering cyberterrorism and its financial support amid the escalation of digital threats to the national security of Ukraine. A doctrinal analysis of the concept of cyberterrorism is carried out through the prism of current national legislation, the draft of the new Criminal Code of Ukraine, and the standards of international law in the field of combating terrorism. Particular attention is focused on the problem of using virtual assets as a means of financing terrorist activity, in view of which the regulatory approaches of the European Union, the recommendations of the Financial Action Task Force on Money Laundering, and the law-enforcement practice of the United Kingdom, the United States, and Australia are analysed. The study also considers emerging cyber-physical threats associated with autonomous distributed platforms, including drone swarms and other multi-agent systems, which may become both targets and instruments of cyberterrorist interference. On the basis of the conducted study, a number of specific legislative amendments are substantiated to the provisions of Article 258 and Article 258-5 of the current Criminal Code of Ukraine, as well as to Article 7.2.3 and Article 7.2.7 of the draft of the new Criminal Code of Ukraine. In the authors' opinion, implementation of the proposed amendments will contribute to the formation of a comprehensive mechanism of criminal-law response to acts of cyberterrorism in the digital age.

Keywords

cyberterrorist, doctrinal analysis, cyberterrorism, regulating the virtual-assets sector, best regulatory practices

1. Introduction

The transformation of digital technologies into an integral component of social life has given rise to qualitatively new forms of socially dangerous offences, among which cyberterrorism occupies a special place. The distinctive feature of this phenomenon lies in the absence of territorial limitations for its perpetrators: an informational impact on critical infrastructure may be carried out from any point in the world without the physical presence of the offender on the territory of the state against which the criminal offence is committed. These circumstances fundamentally complicate both the detection of such acts and the bringing of guilty persons to criminal liability [1].

At the regulatory level, the existing threat has found its reflection in the Cybersecurity Strategy of Ukraine, approved by Decree of the President of Ukraine of 26 August 2021 No. 447/2021. In particular, the said act expressly names, among the principal threats to cybersecurity, the use by terrorist organisations of cyberspace for committing acts of cyberterrorism, as well as financial and other support of terrorist activity [2]. Among the priority targets of cyberterrorist offences, the Strategy includes nuclear power enterprises, electricity- and water-supply systems, the sphere of electronic

CMiGIN'26: Fifth International Workshop on Conflict Management in Global Information Networks, June 26–27, 2026, Krakow, Poland

*Corresponding author.

† These authors contributed equally.

✉ vladyslav.kubalskiy@gmail.com (V. Kubalskyi); kasyanov@i.ua (P. Kasyanov); kysilmaksym@gmail.com (M. Kysil)

ORCID 0000-0001-6127-5786 (V. Kubalskyi); 0000-0002-6662-0160 (P. Kasyanov); 0009-0001-2981-189X (M. Kysil)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

communications, the financial and banking sector, aviation and railway transport, facilities for the storage of strategic types of raw materials, and also chemically and biologically hazardous enterprises.

The armed aggression of the Russian Federation against Ukraine has radically changed the security landscape and demonstrated that the threat of cyberterrorism is not a theoretical concept but a real, everyday danger. In this context, relevance attaches not only to the question of an adequate substantive-law response to acts of cyberterrorism, but also to the problem of neutralising the financial flows that feed them. The digitalisation of financial services has generated a parallel trend: terrorist organisations increasingly actively adapt virtual assets for the collection, transfer, and legalisation of funds, circumventing the traditional mechanisms of banking supervision.

The scale of the said problem is evidenced by the aggregated statistical data of analytical institutions. Thus, according to the monitoring carried out by the analytical company Chainalysis, referred to by the Basel Institute on Governance, during 2021 the total volume of funds received by cryptocurrency addresses associated with unlawful activity exceeded USD 14 billion [3]. For Ukraine, the problem acquired particular acuteness from the moment of the full-scale invasion: journalistic investigations recorded instances of financing of Russian occupation formations through virtual assets in the amount of approximately USD 4.2 million [4].

The aim of this article is to formulate a set of legislative proposals directed at the effective criminalisation of acts of cyberterrorism and their financial support in the Criminal Code of Ukraine (hereinafter - the CC of Ukraine) and the draft of the new Criminal Code of Ukraine. Achieving the stated aim involves solving the following tasks: 1) to disclose the doctrinal content of the concept of cyberterrorism and to substantiate the need for its criminalisation; 2) to analyse relevant foreign experience and to identify models of criminalisation acceptable for Ukraine; 3) to examine the international standards for regulating the circulation of virtual assets in the part concerning countering the financing of terrorism; 4) to formulate concrete proposals for improving national criminal legislation.

2. Analysis of previous research

The problem of cyberterrorism as a socio-legal phenomenon has been addressed in the works of a considerable range of domestic researchers, among whom it is worth mentioning D. S. Azarov, R. O. Bank, O. V. Boichenko, S. A. Buiadzy, L. Yu. Veselova, S. B. Havrysh, O. O. Hrytsun, M. V. Hutsaliuk, V. O. Holubiev, O. D. Dovhan, I. M. Dronin, M. V. Karchevskiy, Yu. I. Kohut, O. Ye. Korystin, B. D. Leonov, S. Ya. Lykhova, O. O. Onchurova, and others. At the same time, a comprehensive analysis of cyberterrorism in its interconnection with the mechanisms of its financial support through virtual assets has not hitherto been carried out in the domestic doctrine, which determines the relevance of the chosen subject matter.

Publications by international-level analytical structures - the Basel Institute on Governance, Europol, the United Nations Office on Drugs and Crime, and the Financial Action Task Force on Money Laundering (hereinafter - FATF) - as well as reports of the House of Commons of the United Kingdom and of the UK Treasury, are devoted to the study of the legal status of virtual assets and of the possibilities of their use in criminal activity. In a joint report of Europol and the Basel Institute on Governance, attention is drawn to the fact that the asset-recovery mechanisms in force in certain jurisdictions, based both on convictions and on non-conviction-based confiscation procedures, have already made it possible to seize significant volumes of virtual assets of criminal origin [5].

3. Doctrinal and criminological dimensions of cyberterrorism

The delimitation of the concepts of 'cybercrime' and 'cyberterrorism' has not only theoretical but also direct practical significance for establishing the limits of the criminal-law prohibition. A cyberterrorist, unlike the subject of a classical terrorist act, does not resort to firearms, explosive devices, or other means of physical impact. Their arsenal is formed by software and hardware means of unauthorised access to information systems, malicious software, and also technologies for remotely affecting the

digital resources of the target of the offence [6]. Such a shift of the method of committing the offence into the virtual plane gives rise to specific difficulties for law enforcement - ranging from problems of fixing the traces of the crime to questions of jurisdiction. The rapid development of autonomous cyber-physical platforms further expands the potential technological environment of cyberterrorism [7]. In particular, drone swarms and other multi-agent systems rely on distributed communication, coordination, navigation, and decision-making mechanisms, making them potentially vulnerable to unlawful interference with communication channels, control algorithms, or coordination protocols. Such interference may result not only in disruption of information processes but also in direct physical consequences where autonomous systems operate in critical, civilian, or defence environments.

In the Ukrainian-language doctrine, the construction of the correlation of the said concepts as generic and specific has been substantiated. In particular, L. Yu. Veselova holds the position according to which cybercrime encompasses the totality of offences in the information and telecommunications sphere, where technologies may act as the object, the environment, or the instrument of the unlawful act; cyberterrorism, within this category, constitutes a specific subgroup distinguished primarily by its political motivation and by its purposefulness in intimidating the population, violating public security, or influencing public authorities [8]. The legal definition of cyberterrorism, enshrined in paragraph 13 of part 1 of Article 1 of the Law of Ukraine 'On the Basic Principles of Ensuring the Cybersecurity of Ukraine' of 5 October 2017 No. 2163-VIII, defines it as terrorist activity carried out in cyberspace or with its use [9]. However, this definition is of a purely general character and is devoid of a criminal law dimension: it contains neither indications of specific acts nor sanctions, without which it is impossible to bring a person to criminal liability.

Cyberterrorist offences carried out from the territory of the Russian Federation or with its direct assistance demonstrate a clearly expressed strategic orientation towards achieving the geopolitical goals of the aggressor state. This manifests itself, in particular, in the destabilisation of the functioning of national critical infrastructure, the discrediting of Ukraine at the international level, and also in the conduct of large-scale information and psychological operations. A textbook example remains the cyberattack using the NotPetya malicious software in 2017, the consequences of which extended far beyond the borders of Ukraine.

Official data of the Security Service of Ukraine attest to the systematic nature of such offences. According to the published information, the 'Armageddon' grouping, identified as a project of the FSB of the Russian Federation, over a prolonged period carried out more than 5,000 cyberattacks aimed, among other things, at infecting approximately 1,500 governmental computer systems [10]. The principal directions of the malefactors' activity have been determined as: gaining control over critical infrastructure facilities (power plants, heat- and water-supply systems); the theft and collection of restricted-access information, primarily in the security and defence sectors; the conduct of information and psychological operations; and the blocking of information systems.

The legal assessment of the said acts within the coordinate system of international law in the field of combating terrorism presupposes taking into account the criteria enshrined in the anti-terrorist conventions ratified by Ukraine. According to these standards, for a socially dangerous act to be classified within the category of terrorist criminal offences, the presence of a terrorist purpose is necessary – the intimidation of the population in order to influence decision-making by public authorities or international organisations. Where such a purpose is established in the actions of the subject of a cyberattack, the corresponding offence must be qualified precisely as an act of terrorism, notwithstanding the fact that information and telecommunications systems act as the means of its commission.

The theoretical substantiation of the expediency of criminalising cyberterrorist offences relies on the criteria of law-making generally recognised in the science of criminal law. The first group of such criteria - the social and the socio-psychological – traditionally includes: the social danger of the act as a mandatory precondition of criminalisation; the relative prevalence of the corresponding offences; the proportionality of the positive and negative consequences of establishing criminal liability; and the impossibility of effectively responding to the offence by means outside the bounds of criminal law [11]. An analysis of cyberterrorism in the light of the cited criteria attests that this phenomenon corresponds to each of them: it is characterised by an exceptionally high degree of social danger (a potential threat

to human life, to critical infrastructure facilities, and to national security), it has a tendency to grow, it cannot be effectively overcome by methods of administrative or civil-law response, and it therefore requires precisely a criminal-law prohibition. The said approach is also reflected in domestic scholarly literature [12].

4. International experience of criminalising cyberterrorist offences

A comparative legal study attests to the existence of several fundamentally distinct models of criminalising cyberterrorism, which may conventionally be classified into the special and the integral. The first model provides for the separation of cyberterrorism into an independent norm of the Special Part of the criminal law, which is typical of the legislation of Georgia and of certain states of the USA. The second - the integral model - consists in expanding the list of methods of committing a terrorist act by supplementing the corresponding general norm with the feature of impact on information and telecommunications systems; this model has been chosen, in particular, by the Republic of Estonia.

According to Article 324¹ of Chapter 11 'Crimes against the State' of the Criminal Code of Georgia, cyberterrorism is recognised as the unlawful taking of computer information protected by law, its use, or the threat of its use, which create the danger of grave consequences ensuing, committed with the purpose of intimidating the population and/or influencing a body of power [13]. An analysis of the said norm makes it possible to single out its key features: the subject matter is computer information protected by law; the objective side includes, alternatively, three variants of conduct - taking, use, or the threat of use; the presence of a risk of grave consequences ensuing is mandatory; and the subjective side is characterised by a special purpose - the intimidation of the population or influence on a body of power.

The integral approach of the Republic of Estonia has found reflection in Article 237 'Acts of terrorism' of Chapter 3 'Criminal offences against state authority' of the Penal Code. In the corresponding norm, among the list of alternative methods of committing a terrorist act, interference with computer data or the hindering of the functioning of computer systems, as well as the threat of committing such actions, is expressly named - on the condition that they are carried out with the purpose of coercing a state or an international organisation into action or inaction. Such acts are punishable by deprivation of liberty for a term of five to twenty years or by life imprisonment [14].

The pan-European tendency consists in the increasing coverage by the criminal-law prohibition of the entire spectrum of forms of terrorist activity, including cyberterrorism, which is conditioned by the awareness of the transnational character of the corresponding threats [15]. An analysis of the practice of the member states of the European Union makes it possible to assert that the integral model of criminalisation, under which cyberterrorist acts are encompassed by an expanded list of alternative methods of committing a terrorist act, is acquiring the status of the dominant one.

5. Countering the financing of cyberterrorism through virtual assets

Countering terrorism has always been inextricably linked with countering its financial support. In modern conditions, terrorist structures have substantially transformed their financial operations, increasingly broadly involving virtual assets (primarily cryptocurrencies) as a means of collecting and moving funds. This tendency allows offenders effectively to circumvent the mechanisms of banking supervision that have developed within the traditional financial system.

Empirical studies confirm the active use by terrorist organisations of cryptocurrencies for collecting donations [16]. Precedent-setting significance was acquired by the operation of the US Department of Justice, conducted in August 2020, which resulted in the largest seizure in history of virtual assets connected with the financing of terrorism. In the course of the operation, the financial campaigns conducted by the 'al-Qassam Brigades' (the military wing of Hamas), 'al-Qaeda', and the 'Islamic State' (ISIS) were dismantled [17]. The exposed schemes were based on the use of digital instruments for accumulating donations of a global character.

5.1. Systemic challenges in regulating the virtual-assets sector

One of the key systemic challenges in regulating virtual assets is the absence of a unified global approach. According to FATF data, national regulatory strategies demonstrate considerable variability - from the introduction of special legal regimes to the complete prohibition of the circulation of virtual assets in certain jurisdictions [18]. The dominant tendency remains the absence of specialised regulation, which forms substantial gaps in the global system of countering the financing of criminally unlawful activity. FATF's statistical indicators confirm the following: as of March 2022, of the 98 jurisdictions that provided information, only 29 had implemented the corresponding regulatory legal acts, and even in these jurisdictions practical law enforcement frequently lacks a systematic character [19].

A direct consequence of the outlined regulatory gaps has been the widespread use of virtual assets as an instrument for financing transnational crime, including terrorism. Although the aggregated public data on the volumes of financing of terrorist organisations by means of cryptocurrencies remain limited, the available evidence confirms their active use of this channel. In particular, it has been established that terrorist networks use specialised online platforms for collecting funds through crowdfunding and anonymous donations, purposefully circumventing the control mechanisms inherent in the traditional banking sector.

5.2. Systematisation of best regulatory practices

Taking into account the complex character of the identified challenges, the systematisation of best regulatory practices acquires key significance. At the basis of state policy in the corresponding sphere there should lie a risk-oriented approach, according to which countermeasures must be proportionate to the identified threats. According to FATF recommendations, states are obliged to ensure the identification, assessment, and understanding of the risks connected with the activity of providers of services in the sphere of virtual assets (Virtual Asset Service Providers, hereinafter - VASP). Indicative in this context is the practice of the United Kingdom, where, within the framework of developing a new regulatory regime, a systematic risk analysis was conducted that encompassed not only the classical threats of money laundering and the financing of terrorism, but also the specific risks inherent precisely in virtual assets [20].

The effectiveness of countering crime in the sphere of virtual assets directly correlates with the level of the operational and technical capacity of law enforcement agencies. Awareness of this dependence has led, at the international level, to the initiation of a number of initiatives that provide for public-private partnership. Thus, in 2017 Interpol launched a project to prevent the criminal use of blockchain technology [21], and the United Nations Office on Drugs and Crime in the same year commenced training programmes for law enforcement officers [22]. A characteristic feature of the said initiatives is their implementation in close interaction with industry leaders (in particular, with the company Chainalysis), which ensures the practical orientation of the training process.

The experience of Israel deserves separate attention, which R. V. Lukianchuk justifiably defines as an example of effective countering of the financing of terrorism using virtual assets. As a result of special operations conducted by the National Bureau for Counter Terror Financing of Israel in close interaction with the intelligence service and the analytical company 'Chainalysis', approximately USD 1.7 million in cryptocurrency directed in favour of the Lebanese paramilitary grouping 'Hezbollah' and the Iranian 'Quds Force' was confiscated; from 2021 onwards, 189 accounts on the 'Binance' cryptocurrency exchange previously connected with the terrorist organisations ISIS and Hamas were confiscated, and in April 2023 more than 500,000 shekels (approximately USD 137,870) from 80 accounts on this exchange were seized [23]. As the researcher rightly observes, the effectiveness of such a model of countering is achieved precisely through the combination of three components: a specialised institutional body (the National Bureau), the application of advanced technological solutions for blockchain analysis, and a systematic public-private partnership with leading industry companies.

A separate problem is formed by ensuring the enforcement of court decisions on the confiscation of virtual assets, which is conditioned by their specific properties: their intangible character, high

price volatility, and the cross-border nature of operations. Responding to the said challenges, leading states are creating specialised institutional structures. Examples are the creation by the US Federal Bureau of Investigation of a Virtual Assets Exploitation Unit, specialising in the analysis and seizure of virtual assets, as well as the formation of an analogous unit within the Australian Federal Police [24]. The aforementioned makes it possible to assert that the development of specialised institutional competences of law enforcement agencies is a necessary precondition for the actual enforcement of decisions in cases connected with the circulation of virtual assets.

A separate direction of systemic counteraction is constituted by the improvement of the institution of mutual legal assistance in criminal matters. The effectiveness of applying international treaties for the confiscation of virtual assets was illustrated by the precedent of 2020: at the request of the Government of Brazil and on the basis of a bilateral agreement, the US Department of Justice carried out the seizure of virtual assets in the amount of approximately USD 24 million [25]. The legal framework of international cooperation in the corresponding sphere is not exhausted by bilateral agreements and encompasses multilateral instruments, among which a special place is occupied by the United Nations Convention against Transnational Organized Crime and the Council of Europe Convention on Cybercrime.

5.3. The regulatory response of the european union and the need to harmonise national legislation

The European Union was one of the first subjects of international law to introduce a systemic regulatory response to the challenges of financing criminally unlawful activity by means of the provision of virtual assets. The adopted Fifth Anti-Money Laundering Directive extended the corresponding rules to providers of virtual-asset services, obliging cryptocurrency exchanges and wallet operators to carry out due diligence of clients (by analogy with the Know Your Client principle), to track transactions, and to report suspicious activity. However, as V. Covolo quite justifiably observes, the implementation of the said rules encounters difficulties in connection with the risks of interjurisdictional arbitrage and the complexity of applying traditional property regimes to digital assets in the cross-border dimension [26].

The next step in the formation of the regulatory architecture was the adoption of Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets. In the preamble of this act it is expressly emphasised that the traceability of the corresponding transactions is a key instrument for the prevention, detection, and investigation of facts of financing of organised crime, as well as for the implementation of international sanctions regimes [27].

The state of national regulation, unfortunately, substantially lags behind European standards. Notwithstanding the adoption, back in February 2022, of the specialised Law of Ukraine ‘On Virtual Assets’, this act has not yet entered into force. As a result, regulation in the corresponding sphere is carried out fragmentarily: the Law of Ukraine ‘On Prevention of Corruption’ of 14 October 2014 No. 1700-VII classifies cryptocurrency within the list of intangible assets subject to mandatory declaration [28], likening it to the legal regime of rights to trademarks or copyright; the Law of Ukraine ‘On Prevention and Counteraction to the Legalisation (Laundering) of the Proceeds of Crime, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction’ of 6 December 2019 No. 361-IX operates with the generalised term ‘virtual assets’ without providing a separate definition of the concept of ‘cryptocurrency’ [29], which complicates law enforcement.

The identified empirical evidence of the use by terrorist structures of regulatory gaps in the sphere of the circulation of virtual assets, combined with the systemic legislative response of Ukraine’s international partners, makes pertinent the need for a prompt updating of national legislation. Without recognition, in the provisions of the corresponding criminal-law norms, of the possibility of financing terrorism precisely through virtual assets, effective counteraction to this form of criminal activity will remain limited.

6. Analysis of the legislation of Ukraine and proposals for its reform

An analysis of the current national criminal legislation attests that, on the one hand, cyberterrorism has been recognised at the regulatory level as one of the principal threats to the cybersecurity of Ukraine (the Cybersecurity Strategy of Ukraine), while, on the other hand, the CC of Ukraine lacks an independent norm that would provide for liability precisely for this variety of offences. As a consequence, cyberterrorist acts may be qualified only under the general norm on a terrorist act (Article 258 of the CC of Ukraine), which, in view of the limited list of methods of its commission in the current wording, creates certain difficulties of law enforcement.

Certain positive shifts in the direction of improving the criminal-law basis for countering cyberterrorism are observed in the draft of the new Criminal Code of Ukraine. In particular, in the wording of the draft as of 1 May 2026, Article 7.2.3 'Terrorist act' already contains an indication of 'unlawful interference with the operation of an information system using malicious software or technical means' as one of the methods of committing the corresponding crime [30]. However, even the updated wording does not encompass the entire spectrum of possible cyberterrorist acts and does not comprehensively resolve the problem of differentiating liability for their financing using virtual assets.

6.1. Proposals to the current criminal code of Ukraine concerning the act of cyberterrorism

We consider it expedient that cyberterrorist offences committed on the territory of Ukraine or against its national interests be qualified under Article 258 of the CC of Ukraine, taking into account the specificity of the method of their commission. With the purpose of ensuring the completeness of the coverage, by the criminal-law prohibition, of all forms of cyberterrorism, it is proposed to introduce amendments to the provision of part 1 of Article 258 'Terrorist act' of the current CC of Ukraine. In particular, after the words 'a terrorist act, that is, the use of weapons, the commission of an explosion, arson', this provision should be supplemented with the words 'unlawful impact on information and telecommunications systems'.

The proposed construction is based on the integral model of criminalisation, the advantages of which are: 1) the preservation of the systemic unity of the norms of Chapter IX of the Special Part of the CC of Ukraine; 2) the avoidance of the terminological redundancy observed in the previously proposed definitions of 'cyberterrorism' (to which, in particular, D. S. Azarov justifiably drew attention with regard to the risk of duplicating the content with other corpora delicti [31]); 3) ensuring the flexibility of law enforcement, since a single norm makes it possible to encompass both 'classical' and cyberterrorist forms of offence.

6.2. Proposals to the draft of the new criminal code of Ukraine concerning the act of cyberterrorism

In the draft of the new Criminal Code of Ukraine, we consider it necessary to expand the list of methods of committing a terrorist act. Thus, we propose to supplement Article 7.2.3 of the draft of the new CC of Ukraine ('Terrorist act') with a new paragraph criminalising actions by which a person 'committed a criminal offence in cyberspace and/or with the use of cyberspace'. The proposed wording will ensure the coverage of the maximally broad spectrum of terrorist acts carried out using digital means, and will take into account future technological development, which at present is difficult to foresee.

Implementation of the said proposals will contribute to the formation of an adequate criminal law response to acts of cyberterrorism, will have a certain preventive potential, and will also attest to the legislator's proper understanding of the level of social danger of such acts in the digital age.

6.3. Proposals concerning the criminalisation of the financing of cyberterrorism using virtual assets

The objective need for the regulatory enshrinement of the specificity of the use of virtual assets in the financing of terrorism requires the introduction of targeted amendments to the norms of the CC of Ukraine concerning the financing of terrorist activity.

We consider it expedient to introduce amendments to Article 258-5 'Financing of terrorism' of the current CC of Ukraine by directly including virtual assets in the list of means of such financing. We propose to supplement the provision of part 1 of the said article with a clarification that financial support of terrorist activity includes, among other things, the provision or collection of 'virtual assets'. The proposed novella will ensure legal certainty on the question of qualifying operations with virtual assets directed in favour of terrorist organisations, and will eliminate the possibility of interpreting the corresponding actions as ones that are formally not encompassed by the current provision.

For the draft of the new Criminal Code of Ukraine, we propose to supplement Article 7.2.7 'Financing and other support of terrorism' - namely, after the words 'A person who provided funds, material means...' - with the words 'virtual assets'. Implementation of the said proposal will ensure the consistency of the updated domestic criminal legislation with current international standards, in particular with the recommendations of FATF and the provisions of Regulation (EU) 2023/1113.

It should be emphasised that the effectiveness of the said criminal-law norms will, to a considerable extent, depend on the comprehensiveness of the legislative amendments. Firstly, an urgent need is the immediate entry into force of the Law of Ukraine 'On Virtual Assets' with its subsequent harmonisation with the current acts of the European Union, in particular with the provisions of Regulation (EU) 2023/1113. Secondly, objectively necessary are targeted amendments to the Criminal Procedure Code of Ukraine in the part concerning the development and enshrinement of a detailed procedural mechanism for the detection, fixation, seizure, and subsequent confiscation of virtual assets. Thirdly, relying on the successful experience of the USA and Australia, it is expedient to consider the question of creating, within the structure of the National Police of Ukraine and/or the Bureau of Economic Security of Ukraine, specialised units whose activity should be focused on the analysis of blockchain transactions and on the conduct of operational and investigative measures and investigative (search) actions in the digital environment.

7. Conclusions

The conducted study has attested that cyberterrorism constitutes a serious threat to the national security of Ukraine, which requires a separate criminal-law response. The financing of this activity has evolved, and virtual assets have become a powerful instrument of terrorist organisations. Although the draft of the new Criminal Code of Ukraine deserves a generally positive assessment, significant gaps remain in it in the criminalisation of the entire spectrum of cyberterrorist acts, in particular their financing using the latest technological means.

The proposed legislative amendments to the CC of Ukraine for combating the act of cyberterrorism include the following:

1. It is proposed to introduce amendments to the current CC of Ukraine to the provision of part 1 of Article 258 ('Terrorist act'), supplementing the list of acts with the phrase 'unlawful impact on information and telecommunications systems'.
2. In the draft of the new Criminal Code of Ukraine, it is proposed to supplement Article 7.2.3 ('Terrorist act') with a new paragraph criminalising actions by which a person 'committed a criminal offence in cyberspace and/or with the use of cyberspace'. The aforementioned is intended to create a broad provision that will encompass any terrorist activity carried out by means of digital tools.

To counter the financial support of acts of terrorism, the following legislative amendments concerning the financing of terrorism are proposed:

1. It is proposed to introduce amendments to the current Criminal Code of Ukraine to Article 258-5 ('Financing of terrorism'), including virtual assets therein. The provision of part 1 should be supplemented with a clarification that financial support includes the provision or collection of 'virtual assets'.
2. For the draft of the new Criminal Code of Ukraine, it is proposed to supplement Article 7.2.7 ('Financing and other support of terrorism') after the words 'A person who provided funds, material means...' with the words 'virtual assets'.

The effectiveness of these criminal-law norms will depend on the further development of special legislation in this sphere and on the improvement of the regulatory legal framework in the sphere of virtual assets, on the enhancement of the technical capacity of law enforcement agencies, and on the deepening of international cooperation. By applying a comprehensive approach, Ukraine is capable of developing a resilient system of legal protection of its national cybersecurity in the digital age.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] V. N. Kubalskyi, Problems of criminalising cyberterrorist offences, *Pravova Derzhava* (2022) 488–497. doi:10.33663/1563-3349-2022-33-488-497, in Ukrainian.
- [2] President of Ukraine, Cybersecurity strategy of Ukraine, 2021. URL: <https://www.president.gov.ua/documents/4472021-40013>, approved by Decree of the President of Ukraine No. 447/2021, August 26, 2021. In Ukrainian.
- [3] Basel Institute on Governance, Crypto asset recovery – scope, laws, and cooperation, 2022. URL: <https://baselgovernance.org/blog/crypto-asset-recovery-qa-part-1-scope-laws-and-cooperation>.
- [4] WIRED, The fight to cut off the crypto fueling Russia's Ukraine invasion, 2022. URL: <https://www.wired.com/story/russia-ukraine-cryptocurrency-funding>.
- [5] Europol and Basel Institute on Governance, Seizing the opportunity: 5 recommendations for crypto assets-related crime, 2022. URL: https://baselgovernance.org/sites/default/files/202212/2022_Recommendations_Joint_Working_Group_on_Criminal_Finances_and_Cryptocurrencies.pdf.
- [6] O. D. Dovhan, I. M. Dronin, Escalation of Cyberthreats to the National Interests of Ukraine and Legal Aspects of Cyberdefence, ArtEk Publishing House, Kyiv, 2017. Monograph. In Ukrainian.
- [7] M. Zgurovsky, P. Kasyanov, N. Pankratova, Y. Zaychenko, I. Savchenko, T. Shovkoplyas, L. Paliichuk, A. Tytarenko, Cognitive ai platform for autonomous navigation of distributed multi-agent systems, *System Research and Information Technologies* (2025) 7–18. doi:10.20535/SRIT.2308-8893.2025.3.01.
- [8] L. Y. Veselova, Administrative-Legal Foundations of Cybersecurity in the Conditions of Hybrid War, Ph.D. thesis, Odesa, 2021. Doctor of Law dissertation. In Ukrainian.
- [9] Verkhovna Rada of Ukraine, On the basic principles of ensuring the cybersecurity of Ukraine, 2017. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>, law of Ukraine No. 2163-VIII, October 5, 2017. In Ukrainian.
- [10] Security Service of Ukraine, The ssu has identified fsb hackers who carried out more than 5,000 cyberattacks on state bodies of Ukraine, 2022. URL: <https://ssu.gov.ua/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-naderzhavni-orhany-ukrainy>, in Ukrainian.
- [11] L. P. Brych, V. O. Navrotskyi, Criminal-Legal Qualification of Tax Evasion in Ukraine, Atika, Kyiv, 2000. Monograph. In Ukrainian.
- [12] Y. I. Kohut, Countering Cyberterrorism as a Threat to the Information Security of Ukraine, Ph.D. thesis, Kyiv, 2021. Candidate of Law dissertation, specialty 21.07.01. In Ukrainian.

- [13] Government of Georgia, Criminal code of georgia, 1999. URL: <https://legislationline.org/sites/default/files/2025-03/Georgia%20English.pdf>, as amended in 2025.
- [14] Republic of Estonia, Penal code of the republic of estonia, 2001. URL: <https://legislationline.org/sites/default/files/2025-03/529122024005.pdf>, amended in 2025.
- [15] V. N. Kubalskyi, Criminal-Legal Problems of Countering Terrorism in Ukraine, Ph.D. thesis, Kyiv, 2007. Candidate of Law dissertation, specialty 12.00.08. In Ukrainian.
- [16] RAND Corporation, National Security Implications of Virtual Currency, Technical Report, RAND Corporation, 2015. URL: https://www.smallake.kr/wp-content/uploads/2016/02/RAND_RR1231.pdf.
- [17] U.S. Department of Justice, Report of the Attorney General's Cyber Digital Task Force, Technical Report, U.S. Department of Justice, 2020. URL: <https://www.justice.gov/archives/ag/page/file/1326061/download>.
- [18] Financial Action Task Force, Virtual assets: What, when, how?, FATF booklet, ??? URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/brochures/FATF-Booklet_VA.pdf.
- [19] Financial Action Task Force, Targeted update on implementation of fatf's standards on vas and vasp, 2022. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtualassets-vasps.html>.
- [20] House of Commons Library, Cryptocurrencies, Research Briefing, House of Commons Library, 2023. URL: <https://researchbriefings.files.parliament.uk/documents/CBP-8780/CBP-8780.pdf>.
- [21] Interpol, Project to prevent criminal use of blockchain technology launched by international consortium, 2017. URL: <https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2017/Project-to-preventcriminal-use-of-blockchain-technology-launched-by-international-consortium>.
- [22] United Nations Office on Drugs and Crime, Unodc launches training to tackle cryptocurrency enabled organized crime, 2017. URL: <https://www.unodc.org/unodc/en/frontpage/2017/May/unodc-launchestraining-to-tackle-money-laundering-and-bitcoin-banking-fraud.html>.
- [23] R. V. Lukianchuk, Countering the financing of terrorism using cryptocurrencies, *Informatsiia i Pravo* (2023) 164–175. URL: <https://il.ippi.org.ua/article/view/287248/281162>. doi:10.37750/2616-6798.2023.3(46), in Ukrainian.
- [24] A. De Kretser, Australian federal police forms cryptocurrency unit to hit criminals, *Financial Review*, 2022. URL: <https://www.afr.com/companies/financial-services/australian-federal-police-formscryptocurrency-unit-to-hit-criminals-20220901-p5bejr>.
- [25] U.S. Department of Justice, Us seizes virtual currencies valued at usd 24 million assisting brazil in major internet fraud investigation, 2020. URL: <https://www.justice.gov/opa/pr/us-seizes-virtualcurrencies-valued-24-million-assisting-brazil-major-internet-fraud>.
- [26] V. Covolo, The eu response to criminal misuse of cryptocurrencies: The young, already outdated 5th anti-money laundering directive (2020). URL: <https://doi.org/10.1163/15718174-bja10003>. doi:10.1163/15718174-bja10003.
- [27] European Parliament and Council of the European Union, Regulation (eu) 2023/1113 of the european parliament and of the council of 31 may 2023 on information accompanying transfers of funds and certain crypto-assets and amending directive (eu) 2015/849, 2023. URL: <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng>.
- [28] Verkhovna Rada of Ukraine, On prevention of corruption, 2014. URL: <https://zakon.rada.gov.ua/laws/show/1700-18#Text>, law of Ukraine No. 1700-VII, October 14, 2014. In Ukrainian.
- [29] Verkhovna Rada of Ukraine, On prevention and counteraction to the legalisation (laundering) of the proceeds of crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, 2019. URL: <https://zakon.rada.gov.ua/laws/show/361-20#Text>, law of Ukraine No. 361-IX, December 6, 2019. In Ukrainian.
- [30] Working Group on the Reform of Criminal Legislation of Ukraine, Criminal code of ukraine (draft): Control text as of 01.05.2026, 2026. URL: <https://newcriminalcode.org.ua/upload/media/2026/05/02/00000-kontrolnyj-proyekt-kk-01-05-2026.pdf>, in Ukrainian.
- [31] D. S. Azarov, Criminal Liability for Crimes in the Sphere of Computer Information, Ph.D. thesis, Kyiv, 2003. Candidate of Law dissertation, specialty 12.00.08. In Ukrainian.