Vol. 11, No. 2, 2025

UDC 004.056.5:32.019.5(4-672ЄС)

https://doi.org/10.23939/shv2025.02.023

CYBER-JIHAD AS A SECURITY THREAT: PECULIARITIES OF USE AND COUNTERACTION WITHIN THE EUROPEAN UNION

Lesia Dorosh
Lviv Polytechnic National University
ORCID: 0000-0001-8558-8525
lesia.o.dorosh@lpnu.ua

Inna Mykhalchuk
Lviv Polytechnic National University
ORCID: 0009-0004-8231-9089
inna.mykhalchuk.mmvmv.2024@lpnu.ua

(Received: 11.02.2025. Accepted: 16.07.2025)

The authors argue that the impact of globalisation on the transformation of traditional threats to the international community caused the emergence of new asymmetric threats. The newest asymmetric threats come from "weak" states or groups, in various ways, which, without military superiority, are able to cause significant damage to stronger international actors. In the article is analysed the main characteristics of asymmetric threats, including their intensity, probability and timeframe, which allow weaker actors to inflict damage. There fore the key tools of such threats are technologies and cyber weapons, in particular the importance of "media terror". "Cyber-jihad" became a part of the Islamic State's (IS) recruitment and radicalisation strategy, in particular through digital platforms such as Telegram and TikTok. Using video games and social media is an important means of propaganda to attract young people. IS' strategies for changing its media campaigns for an international audience, in particular by mixing real acts of violence with elements of virtual mass consumption culture. The difficulty of countering such threats lays in their digital nature and the possibility of anonymous dissemination of materials through secure platforms. The key mechanisms at the EU level that have been established in response to the growing use of social media by jihadist groups for recruitment, propaganda and glorification of violence, are analysed by the athours. These include the European Union Internet Referral Unit, the European Counter-Terrorism Center, and the Digital Services Act, which complements the Digital Markets Act and together form the EU Digital Services Package. It seems that research into the effectiveness of international, regional, and national mechanisms to combat IS' use of cyberspace is very promising.

Key words: *asymmetric threat, cyber-jihad, Islamic State (IS), social media, the EU, security.*

КІБЕРДЖИХАД ЯК БЕЗПЕКОВА ЗАГРОЗА: ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТА ПРОТИДІЯ У МЕЖАХ ЄВРОПЕЙСЬКОГО СОЮЗУ

Леся Дорош
Національний університет "Львівська політехніка"
lesia.o.dorosh@lpnu.ua
Researcher ID R-1453-2017
Author ID: 57203322074

Інна Михальчук
Національний університет “Львівська політехніка”
inna.mykhalchuk.mmvmv.2024@lpnu.ua
ORCID ID: 0009-0004-8231-9089

(Отримано: 11.02.2025. Прийнято: 16.07.2025)

Автори статті аналізують вплив глобалізації на трансформацію традиційних загроз міжнародному співтовариству, які провокують появу новітніх асиметричних загроз. Новітні асиметричні загрози походять від “слабких” у різних розуміннях держав або груп, які, не маючи військової переваги, здатні завдати значної шкоди сильнішим міжнародним акторам. Основними характеристиками асиметричних загроз, зокрема, є їхня інтенсивність, імовірність та часові межі, які дають змогу слабшим сторонам завдавати шкоди. Зазначено, що ключовими інструментами таких загроз є технології та кіберзброя, зокрема підкреслюється значення “медіатерору”. Розглянуто феномен “кіберджихаду”, який став частиною стратегії “Ісламської держави” (ІД) з вербування та радикалізації прихильників, зокрема через цифрові платформи, такі як Telegram та TikTok. Зазначено, що використання відеоігор та соціальних мереж є важливим засобом пропаганди для залучення молоді. Описано стратегії ІД щодо зміни своїх медіакампаній для міжнародної аудиторії, зокрема способом поєднання реальних актів насильства з елементами віртуальної культури масового споживання. Зроблено припущення, що складність протидії таким загрозам полягає в їхній цифровій природі та можливості анонімного поширення матеріалів через захищені платформи. Проаналізовано ключові механізми на рівні ЄС, які створено у відповідь на зростання використання соціальних медіа групами джихадистів для вербування, пропаганди та пропагування насильства. Йдеться про Відділ надання послуг в інтернеті ЄС (European Union Internet Referral Unit), про Європейський контртерористичний центр (European Counter-Terrorism Center), про Закон про цифрові послуги (Digital Services Act), який доповнює Закон про цифрові ринки (Digital Markets Act), і разом вони утворюють Пакет цифрових послуг ЄС (EU Digital Services Package). Наголошено, що перспективним є дослідження ефективності міжнародних, регіональних і національних механізмів для боротьби з використанням ІД кіберпростору.

Ключові слова: *асиметрична загроза, кіберджихад, “Ісламська держава”, соціальні медіа, ЄС, безпека.*

The security situation in the world remains complex and multifaceted, as along with traditional threats such as interstate conflicts, terrorism and armed conflicts, non-traditional challenges are becoming increasingly important. Among them, cyber threats, information attacks, hybrid operations, and the spread of disinformation occupy a special place. These threats are largely driven by the rapid development of information and digital technologies, which have opened up new opportunities to influence states, societies and individuals. The adoption of digital platforms and technologies by jihadist organizations like Islamic State (IS) has reshaped conventional ideas of terrorism into asymmetric threats, particularly through what is termed ‘cyber-jihad’. This trend uses encrypted messaging apps, social media platforms and transmedia stories to recruit, incite radicalisation and coordinate terrorist activities on a global scale to spread ideology and instability, increase influence, attract resources and support A significant research challenge is to comprehend and counteract the changing role of digital networks in fostering these asymmetric threats. The pehomena of cyber-jihad exemplifies how globalization and digital advancements have altered security frameworks, rendering threats harder to anticipate and address. The utilization of platforms like Telegram, TikTok, and narrative-driven gaming highlights the advanced nature of these tactics in exploiting psychological, cultural, and technological weaknesses. Tackling this issue is essential for establishing a robust legal framework, enhancing international collaboration, and formulating innovative counterterrorism approaches that reconcile security with the safeguarding of fundamental rights.

The purpose of the research is to examine the peculiarities of the use of digital platforms by terrorist organisations and to analyse the key mechanisms at the EU level that have been established in response to the growing use of social media by jihadist groups for recruitment, propaganda and glorification of violence.

Source base of the research. The ongoing conflict between Israel and Hamas has heightened tensions and exacerbated the existing jihadist threat, with potential consequences for Europe and the West. Therefore, jihadism in its online manifestation is more relevant than ever as a subject of research and analysis in political discourse. Regulations and official information from various international institutions, mainly European ones, are the main sources for understanding institutional mechanisms for countering cyberterrorism and coordinating joint efforts. This includes legal acts and institutions such as the EU’s Digital Services Act, EU Internet Referral Unit, European Counter Terrorism Centre, Europol and TikTok collaborate to bolster efforts against terrorist content [European Commission 2024; Europol 2022]. The following studies are particularly noteworthy, such as European Counter Terrorism Centre’s paper “The ‘jihadi Wolf’ Threat the Evolution of Terror Narratives Between the (Cyber-) social Ecosystem and Self-Radicalization ‘ego-System’ [Europol 2017]. Scholarly articles and research are also an important source for understanding the theoretical and practical aspects of modern manifestations of terrorism. Such sources offer detailed analysis and critical assessment of new security threats such as asymmetric threats and cyber-jihadism. Among them are studies by such authors as Dr. Bahaa Al-Sabri, J. Babanoury and C. Schaer [Al-Sabri 2023; Babanoury 2024; Schaer 2024]. The works of the following authors made it possible to trace the dynamics of the use of social

networks, including the creation of narratives using characteristic textual and visual elements for propaganda and recruitment: Q. Yuanbo, P. Las Heras, S.Rakhma, P. Widodo and A. H. Sulistyono Reksoprodjo [Yuanbo 2024; Las Heras 2022; Rakhma, Widodo, and Sulistyono Reksoprodjo 2024].

***

Globalization processes are making adjustments to the understanding of traditional threats, the nature of their impact and consequences. Along with traditional threats, new asymmetric threats are coming to the fore. Asymmetric threats are actions taken by weaker states or groups to harm or obstruct stronger states, despite their lesser power. These threats are considered security risks when their purpose is to harm or undermine a state. The main characteristics of an asymmetric threat are severity, probability, and time [Al-Sabri 2023]. This approach allows weaker parties to inflict significant damage even though they lack conventional force, making it the ‘weapon of the weak. The stronger state faces an unpredictable and unclear threat, which makes it difficult to assess potential damage.

Asymmetric threats are difficult to identify due to their vague nature, and they can quickly shift from subjective to objective perceptions, making it difficult to determine whether a party is a threat. They include a variety of factors and actors, including states, international organization, economic institutions, and individuals. A key tool of asymmetric threats is the use of technology and cyber weapons [Las Heras 2022].

The end of the 20th and beginning of the 21st century is characterized by an important security shift due to the ‘mediamorphosis’ of terrorism, as we rapidly move from an analogue era characterized by hierarchical structures and centralized information dissemination institutions to a digital, interconnected and globalized world. Thus, the digital landscape not only serves as a means of disseminating fear-mongering messages, similar to traditional propaganda tactics, but also becomes what can be called ‘media terror’. This ‘media terror’ operates as an asymmetric weapon in our contemporary globalized context, functioning in all dimensions of the violent interaction between ‘action and representation’ and this is where ‘cyber-jihad’ arises [Europol 2017].

The ‘cyber-jihad’ refers to the worldwide use of the Internet by the Islamic State, which positions itself as a Cyber Caliphate, developing special narratives that encourage hacker groups and individuals around the world to participate in the media fight against the ‘crusaders’ and ultimately become part of the United Cyber Caliphate (UCC). The difference between cyber-jihad and cyber-terrorism is that the former involves the dissemination of information by a terrorist group or individual jihadist, while cyber-terrorism generally refers to ‘hacker attacks’ aimed at waging economic, political and psychological warfare. Currently, cyber-jihad serves mainly as a tool: a resource [Babanoury 2024]. One of the most powerful tools of radical propaganda is media and social media.

While early propaganda primarily targeted Arabic-speaking audiences in the Middle East, IS later shifted its strategy to attract international followers, particularly from Western nations. This shift was marked by the introduction of English-language content, including magazines like ‘Dabiq’ and ‘Rumiyah’, and videos tailored to Western audiences. This strategic adaptation underscored IS’s ambition to operate as a multinational entity [Yuanbo 2024]. In addition to linguistic, the transition from local to international media was both thematic and stylistic. IS has begun using video games to glorify terrorism, suicide bombers, and promotes violence against states or political figures by rewarding virtual success. These games are available in multiple languages to reach a wider audience. IS skilfully combines real-life executions with images from popular video games such as ‘Call of Duty’ and movies ‘Saw’, ‘The Hunger Games’, ‘Sin City’ to create a transmedia narrative. This strategy blurs the line between reality and fiction, desensitizing viewers by making violent acts as familiar as scenes from entertainment media [Las Heras 2022].

The worldwide jihadi movement has undergone changes in its platform usage due to stricter regulations. In the early 2010s, IS primarily used Twitter for recruiting, spreading propaganda, and coordinating attacks. However, as Twitter increased the suspension of IS-affiliated accounts, the organization transitioned to Telegram. This encrypted messaging service provided enhanced privacy and fewer regulations at the time, enabling IS supporters to establish channels and groups for safely sharing propaganda, communicating, and planning attacks [The Soufan Center 2024].

IS has shifted its operations from Twitter to Telegram for organizing PR campaigns, sharing materials such as posters, videos, and statements in private before making them publicly available. Telegram markets itself as a highly secure instant messaging platform due to its implementation of end-to-end encryption, ensuring that all data is encrypted from the beginning to the end of the communication process. The platform boasts over 100 million active users, with the majority hailing from regions in the Middle East, Central and Southeast Asia, as well as Latin America. One of the key features introduced on Telegram is the ability to create both public and private channels. This functionality allows users to set up their own channels to share content with an unlimited number of anonymous followers [Europol 2017].

IS has taken advantage of this feature and manages both public and private channels, facilitating direct communication, group discussions, and the distribution of propaganda. Channels can accommodate as many as 200,000 members, allowing for significant outreach. IS additionally utilizes Telegram bots to automate the sharing of content and to oversee channel activities. Although Telegram has made attempts to eliminate channels associated with terrorism, IS continues to take advantage of the platform’s features [Counter Extremism Project 2024].

On Telegram, various groups exist, each focusing on a specific area of interest. Some groups aim to provoke violence, while others explore theological issues to rationalize such violence and its associated actions. There are also groups that highlight the injustices faced by Muslims globally, along with numerous others focused on military training, including those that instruct on bomb-making or how to execute a terrorist attack [Las Heras 2022]. For instance, the Telegram egram channel ‘Whispers of the Forgotten,’ which is sometimes shared by pro-Islamic groups, disseminates content that encourages radicalization and utilizes RocketChat, a service employed by IS-linked factions worldwide. Furthermore, it conducts a fundraising campaign, providing contact information for individuals interested in discussing their contributions [CYFIRMA 2024].

As of February 2024, Telegram has not fully addressed the threat of terrorist activity on its platform. While some steps have been taken to curb IS activities, the platform is still used for planning attacks, sharing propaganda, and disseminating links to IS propaganda repositories. IS's output has declined since 2019, but its content remains active on Telegram [Elliott 2024].

Nevertheless, IS has embraced the new TikTok platform, realizing that it can be an effective tool to attract the attention of the younger generation. Creating visually appealing content, they developed short videos. Using the keyword 'dawlah', displaying the IS flag with stickers, using nasheeds or song lyrics, creating sarcastic memes, and promoting jihad, death, and suicide all attract the attention of young users. This generation is very active on the platform, and when they are exposed to propaganda, the impact can range from intolerance to support for terrorist acts [Rakhma 2024].

Jihadist organizations have taken advantage of TikTok's child-friendly features to make their propaganda more attractive to younger viewers, especially young girls. In 2019, videos displaying jihadists decorated with hearts and flowers were designed to resonate with traditional gender roles and appeared on specific 'For You' pages. These clips showcased women in burqas holding the Islamic State flag, accompanied by captions such as 'Jihad Lover'. This approach seeks to instil jihadist beliefs in young women, ensuring that future generations support and propagate these ideologies within their families and communities [ibid].

As a result, between March 2023 and March 2024, 470 IS-related court cases were documented, with at least 30 of them involving adolescents or minors; the actual number may be higher due to limited data availability. Furthermore, almost two-thirds of IS-related arrests in Europe during recent incidents involved teenagers, highlighting the growing involvement of young people in extremist activities.

The radicalization of young people can be understood through the consistent message propagated by the IS group: the world is persecuting Muslims, but if you join us, we will be strong together. Adolescents who feel alienated or marginalized and are searching for a sense of belonging or clear guidelines in a complicated world might find this message attractive. Political elements contribute to the increasing number of radicalized youth. The IS group leverages the tensions between Israel and Hamas in Gaza to assert that the rest of the world is against Muslims and that its followers must take revenge. The easy access to videos depicting civilian deaths and devastation in Gaza has a profound effect on young people. Encountering violent media can provoke two main reactions in children: isolation or increased aggressiveness [Schaer 2024].

In 2015, the European Union Internet Referral Unit (EU IRU) was established in response to the increasing use of social media by jihadist groups for recruitment, propaganda and glorification of violence. Its main tasks include providing strategic and operational analysis to support the EU authorities, identifying and sharing terrorist and extremist content with relevant partners, and requesting the removal of online material linked to smuggling networks targeting migrants and refugees [Europol 2024]. Afterwards in January 2016, Europol established the European Counter-Terrorism Center (ECTC) as an operational and expert center to strengthen the EU's response to terrorism. The initiative was born out of the 2015 terrorist attacks, which highlighted the need for greater coordination at the EU level. As the first center of its kind in this framework, the ECTC plays a key role in harmonizing national counterterrorism efforts [Europol, 2024. European counter terrorism centre]. Last year 11 governments participated in the ECTC Voluntary Referral Day aimed at identifying suspicious terrorist and extremist content on the Internet. During this collaborative effort, approximately 2,145 pieces of content were examined and flagged to TikTok for voluntary evaluation against their terms of service. The flagged content included items associated with jihadism, as well as violent right-wing extremism and terrorism, like videos and memes. This Referral Action Day is part of an ongoing collaboration between TikTok, law enforcement agencies, and Europol that seeks to tackle the exploitation of the internet by terrorists, curb online radicalization, and protect fundamental rights [Europol 2022].

In November 2022, the Digital Services Act (DSA) came into force, complementing the Digital Markets Act (DMA), and together they form the EU Digital Services Package, a landmark regulatory framework that is transforming the regulation of the digital landscape by addressing issues such as illegal content, disinformation and algorithmic transparency. The DSA sets a European standard for platform accountability and aims to create a safer, fairer and more trustworthy digital space for users across the EU [European Commission 2024].

Conclusions. We can summarise that cyber-jihadism is the dark side of cyberspace, where technology is used for two main purposes: to conduct malicious cyber activities and to facilitate the scaling up of terrorist activities. Cyberterrorism enhances the influence and reach of terrorist organizations by removing physical barriers and providing a global platform for propaganda, recruitment and ideological reinforcement. Terrorists use cyberspace to gain visibility and recognition, using social media such as Telegram and TikTok to make their existence, tactics and goals widely known. This instils fear in global society and inspires like-minded individuals to join their cause. Young people, in particular, are more susceptible to the influence of extremist ideas spread online.

The European Union has implemented actions to counter cyber jihad, creating the EU Internet Referral Unit to detect and eliminate extremist material, along with the European Counter-Terrorism Centre in to improve coordination efforts. Programs such as the ECTC Voluntary Referral Day and regulatory measures like the Digital Services Act aim to reduce online radicalization by holding platforms accountable and ensuring the removal of illegal content. While these changes are seen as favourable to law enforcement, they have led to a shift in cybercrime activity to more decentralized and encrypted platforms with significantly less oversight, making it harder to detect such threats. In this context, ***is promising to study*** the effectiveness of international, regional and national mechanisms to combat IS's use of cyberspace, as this is just as important as physically confronting its forces and preventing its geographic expansion.

БІБЛІОГРАФІЯ / REFERENCES

Al-Sabri, B. (2023). Asymmetric threats: A study in the transformations of traditional deterrence strategies. ***Strategies. Think Tank.*** Retrieved from https://strategiecs.com/en/ analyses/

asymmetric-threats-a-study-in-the-transformations-of-traditional-deterrence-strategies

Europol. (2017). *The Jihadi Wolf' threat: The evolution of terror narratives between the (cyber-)social ecosystem and self-radicalization 'ego-system'*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/antinoria_thejihadiwolfthreat.pdf

Babanoury, J. (2024). Cyber Jihad: The internet's contribution to Jihad. *Ceis - Incyber News.* Retrieved from https://incyber.org/en/article/cyber-jihad-the-internets-contribution-to-jihad-par-julien-babanoury-ceis/

Counter Extremism Project. (2024). *Terrorists on Telegram*. Retrieved from https://www.counterextremism.com/sites/default/files/2024-02/Terrorists%20on%20Telegram_022024.pdf

CYFIRMA. (2024). *Islamic State's Telegram hustle: How a terrorist organization raises funds*. Retrieved from https://www.cyfirma.com/research/islamic-states-telegram-hustle-how-a-terrorist-organization-raises-funds/

Elliott, V. (2024). Telegram's bans on extremist channels aren't really bans. *WIRED*. Retrieved from https://www.wired.com/story/telegram-hamas-channels-deplatform/

European Commission. (2024). *The EU's Digital Services Act*. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

Europol. (2022). *EU Internet Referral Unit - EU IRU*. Retrieved from https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru

Europol. (2022). *European Counter Terrorism Centre - ECTC*. Retrieved from https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc

Europol. (2022). *Europol and TikTok collaborate to bolster efforts against terrorist content*. Retrieved from https://www.europol.europa.eu/media-press/newsroom/news/europol-and-tiktok-collaborate-to-bolster-efforts-against-terrorist-content

Las Heras, P. (2022). How does ISIS recruit its members*? Global Affairs and Strategic Studies.* Retrieved from https://en.unav.edu/web/global-affairs/como-recluta-el-isis-a-sus-miembros

Rakhma, S., Widodo, P., & Sulistyono Reksoprodjo, A.H. (2024). TikTok and Islamic State of Iraq and Syria (ISIS) Propaganda. *International Journal of Humanities Education and Social Sciences.* Retrieved from https://ijhess.com/index.php/ijhess/article/view/1103/824

Schaer, C. (2024). The teenage terrorists of the 'Islamic State'. *DW*, 9 November. Retrieved from https://www.dw.com/en/the-teenage-terrorists-of-the-islamic-state/a-70182153

The Soufan Center. (2024). *TikTok Jihad: Terrorists leverage modern tools to recruit and radicalize*. Retrieved from https://thesoufancenter.org/intelbrief-2024-august-9/

Yuanbo, Q. (2024). Propaganda in focus: Decoding the media strategy of ISIS. *Humanities and Social Sciences Communications.* Retrieved from https://www.nature.com/articles/s41599-024-03608-y