Research article
DOI: https://doi.org/10.21202/jdtl.2023.10

Terrorist Crimes in the Era of Digitalization: Forms of Activity and Measures for Counteraction

Elena Yu. Antonova

Far East Juridical Institute (branch) of the University of Public Prosecution of the Russian Federation
Vladivostok, Russian Federation

Keywords

Counteraction,
crime,
criminalization,
digital funding,
law,
propaganda,
recruitment,
space,
technologies,
terrorism

Abstract

Objective: to elaborate recommendations on counteraction against terrorist crimes committed in the digital (cyber-) space and/or using digital technologies.

Methods: the methodological basis of the research are the universal dialectic method of cognition, the integrity of general and specific scientific methods such as analysis, synthesis, logical method, ascent from the abstract to the specific, induction, deduction, etc.

Results: it was determined that the development of the digital (cyber-) space and digital technologies promotes the intensity of terrorism and has led to the change of the mechanism of terrorist crimes commitment. A conclusion was made that, to provide the efficiency of measures for counteracting terrorist crimes committed in the digital (cyber-) space and/or using digital technologies, a distinct strategy is necessary, as well as the appropriate regulatory basis.

Scientific novelty: the article analyzes such forms of criminal activities of terrorist groups, committed in the digital (cyber-) space and/or using digital technologies, as dissemination of the ideology of violence and propaganda of terrorist activity, recruiting new members and their training, implementing digital technologies for preparation and immediate terrorist activity, and funding. The advantages were revealed of the use of digital space and/or digital technologies when committing terrorist crimes. In the author's opinion, the change of the mechanism of terrorist crimes commitment associated with the use of digital technologies should be taken into account during criminalization (change of the intensity of penalization) of publicly dangerous deeds.

The important areas of state policy in the sphere of counteraction against these crimes are education and enlightenment activity, training of the personnel of law-enforcement agencies, broadening their authorities to ensure a clear and effective control over digital content.

Practical significance: is due to the possibility to use the formulated conclusions and proposals for further scientific elaboration of the state criminal policy in the sphere of counteraction against terrorist crimes committed in the digital (cyber-) space and/or using digital technologies.

For citation

Antonova, E. Yu. (2023). Terrorist Crimes in the Era of Digitalization: Forms of Activity and Measures for Counteraction. *Journal of Digital Technologies and Law, 1*(1), 251–269. https://doi.org/10.21202/jdtl.2023.10

Contents

Introduction

Crimes in the digital (cyber-) space and/or committed using digital technologies/systems/software are a natural evolution of criminality, determined by the scientific and technological progress and new developments; these crimes represent one of the gravest problems of the contemporary world.

Terrorist crimes are no exception. Notably, the level of terrorism continues growing, as well as "the technological advances that facilitate attracting the attention and emotional impact terrorists seek" (Orehek & Vazeou-Nieuwenhuis, 2014). Researchers register a direct link between the digital (cyber-) space and various forms of social and political destabilization: anti-government demonstrations, unrest and terrorist attacks (Khokhlov & Korotayev, 2022).

Deputy Secretary of the Security Council of Russia Yu. Kokov rightly states that the era of digital terrorism is coming, which, by the scale of probable consequences, may be compared to the weapons of mass extermination. According to his data, there are about 30 thousand terrorist and extremist websites in the Internet[1]. These circumstances require extensive work to counteract terrorist crimes committed in the digital (cyber-) space and/or using digital technologies/systems/software.

1. Forms of criminal activities of terrorist groups committed in the digital (cyber-) space and/or using digital technologies

The persons involved into terrorist activity intensively use modern digital technologies both when committing crimes and in everyday life. Such technologies are used within terrorist communities/organizations (further – groups) as a means of communication, including during organization and management of terrorist activity, and when recruiting new members of terrorist groups, disseminating the ideology of violence, propagating terrorist activity, calling for commitment of certain terrorist acts. Members of terrorist groups strive to broadcast such messages and demonstrate their illegal deeds to the maximally broad audience, as their main goal is to destabilize the society and to decrease its moral and political steadiness.

[1] Security Council of the Russian Federation: digital terrorism can be compared to the weapons of mass extermination. (2022, May 18). *TASS*. https://tass.ru/politika/14658343/amp

1.1. Dissemination of the ideology of violence, propaganda of terrorist activity via digital (cyber-) space

Ideology of violence plays one of the leading roles in committing terrorist crimes (Antonova, 2018). Terrorism is a political tool requiring motivation and skills, which determine its scale, origin, ideology, and counterstrategies (Orehek & Vazeou-Nieuwenhuis, 2014). It is marked that the success of ISIL* depends, inter alia, on "their group functioning as an organization of well-trained, ideologically motivated and merciless warriors" (Makinda, 2016). The Internet became an ungovernable digital space, used, inter alia, for disseminating and cultivating the ideology pf terrorism.

For example, the members of extreme right-wing groups (XRW) use the Internet for conversion into their faith, propagating the atrocities of terrorists and their maximal proclamation, broadcasting their attacks live. For example, of 22 terrorist conspiracies disclosed in Great Britain from March 2017 to September 2019, seven were inspired by XRW ideology. In the same period, persons inspired by XRW ideology committed three terrorist attacks with lethal outcomes (Zedner, 2021). Thus, in the digital era one can be very closely connected to online groups and contacts, which may have similar interests and ideology of violence (Liem et al., 2018), but remain non-member of these groups, acting alone, including with terrorist purposes.

Terrorist groups employ the fact that the digital (cyber-) space allows transmitting information instantaneously, in mere seconds, to an indefinitely broad territory. Via the Internet, mobile devices and social media platforms, a very disturbing and potentially worrying video content can be broadcasted; for example, one may watch international terrorist attacks live, accompanied by shootings and explosions (Huddy et al., 2021). Besides, through the channels of social networks, both official authorities and the broad public react to dangerous situations. The growing use of Twitter** and Facebook*** during emergencies is a bright example of how the public perceives the information loaded in the digital (cyber-) space as "truthful". Although our time is called the epoch of fake news or disinformation, the public still generally trusts information received via the Internet or social networks (Grobbelaar, 2022).

Disseminating via the digital (cyber-) space information which not always correlates with reality (it can be disinformation, rumors, threats of using violence or images of the acts of violence), terrorist groups influence not only the actual or probable supporters of terrorist ideas or the ideology of violence (which is used, first of all, for recruiting new members, radicalization, incitement for terrorism, undermining trust in social values), but also the direct or indirect victims of terrorist attacks (intimidation of the population through psychological manipulation, dissemination of the feelings of increased anxiety, alarm, fear or panic among the population) or the authorities and the international community in general (destabilization of the functioning of authorities or international organizations, or influencing their decisions).

This is also due to the fact that terrorism is interpreted as purposeful use or threatening to use violence by individuals or subnational groups to achieve a political or social goal through intimidation of a large audience, besides the immediate victim (Sandler, 2013). For example, from 2014 to 2017 ISIL* beheaded 296 people and published video recordings of executions of western hostages, including American journalists James Foley and Steven Sotloff, as well as British humanitarian aid workers David Haines and Alan Henning. All four hostages were executed in 2014. In a poll carried out by HuffPost-YouGov in November 2014, 32 % of Americans said that they saw at least several video recordings with beheadings by ISIL*, while 9 % said they saw actual beheading (Schwartz, 2014). According to the data obtained at the national level from a representative online group, polled about six to nine months after the most famous executions in the USA, 25 % of the Americans said they saw some or all videos with beheadings (Redmond et al., 2019). Such actions are aimed, first of all, at intimidation of the population and dissemination of the feelings of increased anxiety and fear, which may lead to panic among the population.

Also, the actions of terrorists are often aimed at provoking reaction of the government, such as territorial cessions or political reforms through acts of intimidation, which exhaust the resoluteness of the opposing government or underline its inefficiency (Kydd & Walter, 2006). That is why terrorist groups strive to adapt extreme communication means to attract attention and visibility in the global media environment (Kraidy, 2018; Nossek, 2008). The violence of terrorists becomes highly mediatized and spectacular, transforming the attacks into media events taking place in a hybrid media environment and rooted in the available technologies (Uusitalo et al., 2021).

To perform propagandist action, terrorist groups often use a broad range of technical means: websites, chat groups and chat forums, online magazines, social media platforms like Twitter** and Facebook***, popular video- and file-sharing sites like YouTube. The Internet search engines simplify the search for terrorist content.

At the hearings in the United States House Homeland Security Subcommittee on Intelligence and Counterterrorism, examples of terrorist using artificial intelligence systems (further – AI) were given. For example, a white supremacist opened fire on two mosques in Christchurch (New Zealand), killing 51 and wounding 49 people. The terrorist managed to broadcast his attack live on Facebook***, because the Facebook AI did not consider the video terrifying enough. Then the video was 300,000 successfully downloaded on Facebook*** by other users. This proves that the AI technologies intended to block such videos do not yet cope with the set task. Moreover, some facts show that the Facebook AI shoots video and promotes terrorist content which it was supposed to remove[2].

[2] Artificial Intelligence and Counterterrorism: Possibilities and Limitations. (2020). *Hearing Before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security House of Representatives One Hundred Sixteenth Congress. First Session. June 25, 2019* (Serial № 116-28). Washington: U.S. Government Publishing Office.

Even if the criminals do not broadcast an attack, witnesses make video recordings which are included in news rills, often uploaded to online sites such as YouTube, as well as to social media platforms such as WhatsApp and Snapchat. This raw graphic video content is readily accessible (sometimes accompanied by a gratuitous warning) and may arouse strong emotions, potentially amplifying public reactions to the terrorist attack (Huddy et al., 2021).

1.2. Recruitment of new members of terrorist groups and their training

Recruitment of new members plays an important role in the functioning of a terrorist group, as the inability to recruit enough members and perform successful attacks testifies to the weakness of the group (Polo, 2020). The development of information-communication technologies, especially the Internet and its tools, provides the platform used by terrorist groups for recruiting new members and disseminating propaganda (Dingji Maza, 2020), as well as for their online training and planning terrorist attacks.

For example, Al-Shabaab using video and Internet messages has made this terrorist organization known worldwide. Before 2009, Al-Shabaab recruited only the Somalis. But after their public connections with Al-Qaeda* were established, foreign militants were recruited, who ideologically identified themselves as the global jihad. One of the most well-known international fighters Omar Hammami, also known as Abu Mansoor al-Amriki, since 2010 regularly published in the Internet messages and disseminated them as Al-Shabaab recruiting (Grobbelaar, 2022).

It is noted that creation of local networks of terrorist groups or joining them facilitates training and knowledge transfer; allows performing joint trainings and attack planning; increases accessibility, delivery and exchange of arms, personnel and other assets related to terrorism; local networks even allow the groups to create alliances, unite and perform coordinated campaigns against the state. Thus, terrorist networks function as a decisive factor, increasing power, maintaining the group potential, their capabilities and efficiency (Polo, 2020).

Besides, specialized terrorist websites act as online libraries of ideological texts, platforms for recruiters and forums for exchanging information. Photo- and video-materials, games (imitating terrorist attacks and encouraging users to participate in role play as a virtual terrorist), manuals and technical instructions, prepared by terrorist groups, promote radicalization of their supporters (Khokhlov & Korotayev, 2022). Propagandist materials may contain ideological or practical guidelines, explanations, justifications, or advertisement of terrorist activity.

For example, when checking the Internet resources, the Shakhunskiy city Prosecutor's office of Nizhegorodskaya oblast, using GoogleChrome browser, by keywords ExpedientHomemadeFirearms in the Yandex search engine received a list of Internet websites with references: <redacted>. The websites contained detailed information about

the techniques of manufacturing weapons and its discussion. The access to the materials is free for all users; the website has no access restriction, no preliminary registration or password is required; any user may see the contents of the website and make an electronic copy of the materials; there are no restrictions on their transmittance, copying or dissemination[3].

As specialists mark, the impact on computer information allows a criminal to "manipulate emotions and mind of a victim, causing grave psycho-physiological consequences. The psycho-physiological effect is comparable by magnitude with the effect of real-world events, while it is modeled by altering computer information" (Dremlyuga, 2022).

Research shows that social movements often use digital media space to work with identification, using digital messages to develop a common sense of "we" (Gaudette et al., 2020). There are significant evidences that social media have become a site for the formation of identities and promote formation of communities with a strong sense of group solidarity (Törnberg & Törnberg, 2022). Terrorist groups employ such psychological techniques when recruiting new members and propagate their ideology.

1.3. Implementing digital technologies in preparation and immediate terrorist activity

Research states phenomenal success of AI systems not only in the sphere of digital platforms bur also in the material environment. This is obvious by the example of introducing digital technologies (robotics) into the controlling system of unmanned vehicles, which simplifies committing terrorist attacks. There are cases of using digital technologies, including unmanned vehicles, in preparatory and immediate terrorist activity, in particular, for delivering drugs, psychoactive substances and other prohibited objects – weapons, explosives, explosive devices, etc.

For example, terrorist groups more and more often use unmanned vehicles for surveillance, explosions and other publicly dangerous deeds both at the stage of preparation and immediate commitment of terrorist attacks. ISIL* announced the use of military drones in Iraq and the creation of an "Unmanned Aircraft of the Mujahideen" division[4]. Also, ISIL conducted several bombing attacks using drones, targeting both civilian and military targets, even attempting drone attacks on heads of state[5]. As production

[3] Archive of Shakhunskiy district court of Nizhegorodskaya oblast. Decision no. 2A-214/2021 of March 22, 2021. Case no. 2A-214/2021. (2021). *Judicial and normative acts of the Russian Federation*. https://sudact.ru/regular/doc/AAQ1OEJsQbb9/

[4] Joby, Warrick. (2017, February 17). Use of weaponized drones by ISIS spurs terrorism fears. *The Washington Post*. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html

[5] Gavin, J. *Trends in Terrorism [2022]*. Vision of Humanity. https://www.visionofhumanity.org/trends-in-terrorism/

of these innovative devices increases and becomes cheaper, terrorists will use them more often. Traditional weapons may still be used but innovative ones will be employed more and more often[6].

3D-printers can make sophisticated and expensive technologies accessible for terrorists. For example, the attacker of a German synagogue on Yom Kippur early October 2019 used 3D-printed components of the home-made weapons[7]. In 2020, a German terrorist spent just $50 to 3D print parts for a gun used in an attempted attack in Halle[8].

The digital (cyber-) space use also used as a means to perform cyber attacks aimed at disturbing the normal functioning of computer systems, servers with computer viruses, malicious software and spyware or other means for illegal access to computer information. These actions are characterized by such features of a terrorist attack as an attempt, by intimidating the population, to destabilize the functioning of authorities or international organizations, influence their decision making, thus achieving political or other social goals.

1.4. Digital channels of terrorism funding

To achieve the set goals and efficient functioning, terrorist groups attract significant material (financial) resources. The digital (cyber-) space and new digital technologies facilitate rapid acquisition of income, further used for the needs of terrorists.

Numerous research show that terrorist groups like Al-Qaeda*, Hamas and mujahedeen, receive funding and support through digital payments from groups and individuals sympathizing with them. Examples of such payments include Internet banking, mobile transfers of money, online commerce and a broader use of cryptocurrencies such as Bitcoin (Dingji Maza et al., 2020). The Head of the CIS Anti-terrorist Center A. Novikov states that "digital transformation of mechanisms and channels of terrorism funding has occurred". As sources of income, terrorists use online casinos, steal money via fake Internet stores and spoof websites, use fishing and farming attacks, unsanctioned access to bank resources and cryptocurrency exchange[9].

6 Noor, E. (2020, January 29). *Sharing space: Tech and terrorism.* Observer Research Foundation. https://www.orfonline.org/expert-speak/sharing-space-tech-terrorism-60862/

7 Beau Jackson. (2019, October 18). "Interview with the ICSR: A 3D printed gun was not used in the Halle terror attack". *3D Printing Industry*. https://3dprintingindustry.com/news/interview-with-the-icsr-a-3d-printed-gun-was-not-used-in-the-halle-terrorattack-163643/

8 Gavin, J. *Trends in Terrorism [2022].* Vision of Humanity. https://www.visionofhumanity.org/trends-in-terrorism/

9 *Terrorists more and more actively use IT technologies, the CIS Anti-terrorist Center says* (2020, March 3). RIA Novosti. https://ria.ru/amp/20200218/1564913906.html

Besides, terrorist groups use the digital (cyber-) space to directly ask for donations. For that, they use websites, chat groups, mass mailing with requests for donations.

For example, North Caucasus District Military Court adjudged Sh., who published in the Internet a call for fund raising for ISIL*. He transferred the money collected to the terrorist group account[10]. In another case, investigation and court stated that M. transferred 7,000 rubles to the account used for raising money for Hay'at Taḥrīr aš-Šām group*, which is a division of the banned terrorist organization Jabhat al-Nusra*[11].

Websites are also used as Internet shops offering books, audio- and video-recordings and other materials with the respective content. Selling such goods allows obtaining additional income and promotes dissemination of terrorist ideology.

2. Advantages of using digital (cyber-) space and/or digital technologies in committing terrorist crimes

The advantages of using digital (cyber-) space and/or digital technologies are due to, first, the high speed of data transmission and information (disinformation) dissemination, as well as of processing of large amounts of information, which allows, for instance, to operatively find supporters, recruit new members of terrorist groups, etc.; second, it is due to the access to an indefinitely broad audience and broadening of the geography of dissemination of the destructive violence ideology under relative anonymity; third, to the difficulty in controlling the conceptual part of the information disseminated; fourth, to the simple coordination of actions of the terrorist groups members.

Besides, the obvious advantages of digital technologies are the possibility to use them in any, including dangerous, territories (zones of military conflicts); physical safety of the subjects using them (when dangerous objects are used – chemical, poisoning or explosive substances, etc.) and difficulty of their discovery (Antonova, 2022).

The above listed and other factors in many cases increase the public danger of the deeds committed, which also should be reflected in the criminal legal norms.

In this respect, the underage are especially attractive for terrorist groups, as having little experience, stable positive orientations and being active users of the digital (cyber-) space. Besides, as is noted in scientific literature, "adolescents are prone to form attitudes for aggressive behavior". The most effective technologies aimed at them are those stirring aggression through extremist slogans, politization of social-economic problems, romantization of the images of negative "heroes", imposing the ideas propagating

[10] *In Dagestan, the court sentenced a man raising funds for Islamic State to 17 years* (2019, August 2). RBK. https://www.rbc.ru/rbcfreenews/5d44544c9a7947190c12566e

[11] *In the Russian Federation, a sentence for funding terrorism is passed*. (2020, September 30). EurasianGroup. https://eurasiangroup.org/ru/sentence-for-terrorist-financing-in-russian-federation34

violence as a social norm and immersing them into destructive internet-communities (Shchetinina, 2018). To recruit the underage, popular musical clips, computer games, cartoons, stories are used, which encourage and praise the actions of terrorists, the missions of suicide attackers, etc.

For example, in October 2019 to June 2020, three 15 year old adolescents "via communication in a social network and messengers, adhering to anarchist ideas… united in a group in order to jointly carry out terrorist activity in the territory of Kansk city". Having distributed roles, the adolescents independently underwent training by reading the prohibited literature, recognized as extremist by the court decision, and watching video films on manufacturing explosive substances and devices in order to carry out terrorist activity. They independently manufactured explosive substances and devices and trained in using them in an abandoned house, waste lots and construction sites in order to get prepared for committing a terrorist attack by exploding a police building or the Agency of Federal Security Service (further – FSS). The case files include screenshots of correspondence in social media, where the defendants discussed where and how to purchase the explosive components. Besides, the schoolboys intended to build a FSS building in Minecraft and to explode it "for visual clarity"[12].

The above is confirmed by the specialists in terrorism counteraction. For example, the Director of Counterterrorist Agency of the United Nations Organization V. Voronkov states that terrorists actively use various technological advances. Using social media and encrypted messages ("darknet"), they spread their hate-crazed ideology, collect and transfer money, radicalize the youth and recruit new supporters, coordinate terrorist attacks. Notably, they use the algorithms of social media in such a way as to quicker and wider disseminate their content. There is information about attempts of the terrorist underworld to use medications to create biological weapons. To deliver chemical, biological or radiological materials, terrorists may use unmanned vehicles, including automated ones[13].

[12] *A teenager from Kansk sentenced to 5 years in a prison camp for preparing a terrorist attack*. (2022, Februry 10). Delovoy Peterburg. https://www.dp.ru/a/2022/02/10/Podrostka_iz_Kanska_prigo

[13] In Minsk, they discuss the capabilities of new technologies and the artificial intelligence in fighting terrorism. (2019, September 3). United Nations Organization: [website]. https://news.un.org/ru/story/2019/09/1362292

3. Counteraction against terrorist crimes committed in the digital (cyber-) space and/or using digital technologies

The difficulty of counteracting against terrorist crimes is, first of all, due to the fact that it "is not subject to clear quantitative measuring; the explanation to this fact is complex: contradictions in the existing normative regulation, imperfection of law enforcement and mechanisms of strategic accounting… innumerability and constantly changing nature of digital crime" (Russkevich et al., 2022).

To counteract terrorist crimes committed in the digital (cyber-) space and/or using digital technologies, it is necessary to elaborate effective mechanisms, including those of criminal-legal character, which would allow timely reacting to terrorist threats in the digital environment.

It should be noted that the difficulties in counteracting publicly dangerous deeds, including terrorist ones committed in digital space, as a rule, leads to changes in normative-legal bases of states. Most often, such changes are related to strengthening the legal liability for committing such deeds.

For example, as the guilty in terrorism are usually individual subjects radicalizing in the Internet, Section 3 of the British Counter Terrorism and Border Security Act 2019 (CTBSA) stipulates criminal liability for nonrecurrent viewing in the Internet of "materials which can be useful for a person committing or preparing a terrorist attack". Such deed entails a maximal punishment of 15 years of imprisonment (Zedner, 2021).

Changes are also being made in the Russian criminal legislation: the norms are complemented with a qualifying (specifically qualifying) sign: "committed with the use of mass media or electronic or informational-telecommunication networks, including the Internet"; norms on crimes in the sphere of computer information are being transformed and new ones appear. Despite all legislative novelties, we still cannot ascertain the presence of appropriate, effective system of criminal-legal measures against persons committing the said crimes in the digital (cyber-) space and/or using digital technologies. Analysis of the criminal legal norms shows that, so far, the Russian legislator has only increased liability for public calls for terrorist activity, public justification of terrorism or propaganda of terrorism (Article 2052), in case they are committed in the digital (cyber-) space (Part 2). All other norms on terrorist crimes lack the relevant qualifying (specifically qualifying) sign. At the same time, practice shows that the digital (cyber-) space is used not only for dissemination of propagandist information for terroristic purposes, but also for facilitating terrorist activity, including recruitment of new members of terrorist groups, funding, training of executors, incitement to committing terrorist attacks, etc.

It should be noted that it is impossible to counteract terrorist crimes committed in the digital (cyber-) space and/or using digital technologies only by criminalizing new publicly dangerous deeds or increasing the intensity of penalization. It is necessary to clearly understand the mechanism of committing such crimes. Hence, new tasks are posed before

law enforcement agencies, which must be able to operatively reveal the source of terrorist threat and block or eliminate it.

Besides, as stated in the scientific literature, rapid development of digital technologies, intellectual devices and social media has decreased the ability of public security services to control the public reaction to a terrorist attack. As the personnel (the services) more and more rely on digital technologies, it is not known how they would act in case of cyber-systems failure. In this regard, the probability of a cascade catastrophe and occurrence of cyber-vulnerability increases (Keenan, 2019). All that can be used by terrorist groups and must be taken into account when elaborating measures for counteracting such crimes.

Conclusions

The carried out analysis of various forms of criminal activity of terrorist groups, committed in the digital (cyber-) space and/or using digital technologies, allows stating that:

1) the development of the digital (cyber-) space (social media, electronic mass media and other Internet resources), the increased number of the users of such space and digital technologies/systems/software facilitates the broadening of violence ideology due to intensive propagandist activity by terrorist groups and, as a result, intensity of terrorism;

2) the use of digital technologies by terrorist groups actually leads to changing the mechanism of terrorist crimes commitment – from the preparation stage to the accomplished crime and suppression of its traces.

These circumstances must also be accounted for when elaborating constructive, effective measures for counteracting terrorist crimes. Modern digital technologies should be more actively used in revealing, disclosing and investigating terrorist crimes, especially if committed in the digital (cyber-) space as well as using IT technologies. An important aspect in this regard is the possibility to use AI by operative-investigation units (for example, facial recognition system, identification of a personality, vehicle numbers, monitoring of social media, etc.).

The digital (cyber-) space may be effectively used for carrying out operative-investigating acts, collecting information extracted from messages in websites, chats and other digital resources, which will facilitate timely prevention and preclusion of terrorist attacks, collecting evidences for bringing the subjects of terrorist activity to criminal liability.

Another countermeasure is creation of websites, chat groups, chat forums and other internet platforms for conducting constructive online discussions, demonstrating counterterrorist and other educational and enlightening materials based on specific facts, for describing alternative non-violent means of solving political and other social problems.

To effectively reveal, disclose and investigate terrorist crimes committed in the digital (cyber-) space and/or using digital technologies, law enforcers must possess not only legal

but also special technical knowledge about the mechanism of such crimes commitment. They must be aware of the modern digital (computer, information and communication) technologies/systems/software, the mechanism and order of their functioning.

Thus, to ensure the efficiency of measures for counteracting terrorist crimes committed in the digital (cyber-) space and/or using digital technologies, a clear strategy and the appropriate regulatory basis is required, which should be aimed at:

1) criminalization (change of the intensity of penalization) of publicly dangerous deeds (including terrorist ones), committed in the digital (cyber-) space and/or using digital technologies. For that, it is necessary to revise criminal law and other regulatory acts in the sphere of digital technologies in order to reveal gaps in the legal protection of objects against terrorist threats and to determine the demand for penalty enhancement in specific cases. Assumingly, commitment of crimes in the digital (cyber-) space and/or using digital technologies may not always increase the degree of public danger of illegal deeds. In this regard, we consider it sufficient, at the present stage, to complement Article 63 of the Russian Criminal Code with Part 12, stipulating it in the following wording: "12. A judge (court) imposing a punishment, depending on the character and degree of public danger of the crime, circumstances of its commitment and a personality of the guilty, may consider commitment of the crime with the use of digital and information-telecommunication technologies to be an aggravating circumstance";

2) enhancement of forces and means for education and enlightenment, including in the digital (cyber-) space, aimed at propagating "peaceful coexistence of all peoples regardless of the race, nationality, language, and origin, as opposed to negative informational-ideological impact on a personality from the outside, including propaganda of the ideology of terrorism" (Ishchuk et al., 2021);

3) training of law enforcers to reveal, disclose and investigate crimes, including terrorist crimes committed in the digital (cyber-) space and/or using digital technologies;

4) broadening the authorities of law enforcers to ensure a clear and effective control over digital content;

5) elaborating international cooperation agreements in the sphere of crime counteraction, including terrorist crimes committed in the digital (cyber-) space and/or using digital technologies.

---

* The organization is recognized as terrorist, its activity is prohibited in the territory of the Russian Federation.

** The social network blocked in the territory of the Russian Federation for disseminating unlawful information.

*** The organization is recognized as extremist, its activity is prohibited in the territory of the Russian Federation.

References

Antonova, E. Yu. (2018). Terrorism as the ideology of violence. *Vestnik Dalnevostochnogo Yuridicheskogo Instituta MVD Rossii*, *2*(43), 69–74. (In Russ.).

Antonova, E. Yu. (2022). Technologies of artificial intelligence – a subject or a tool/means of crime? *Yuridicheskiy vestnik Kubanskogo gosudarstvennogo universiteta*, *1*, 31–39. https://doi.org/10.31429/20785836-14-1-31-39

Dingji Maza, K., Koldaş, U., & Aksit, S. (2020). Challenges of Combating Terrorist Financing in the Lake Chad Region: A Case of Boko Haram. *SAGEOpen*, *10*(2), 215824402093449. https://doi.org/10.1177/2158244020934494

Dremlyuga, R. I. (2022). *Criminal-legal protection of digital economy and informational society against cyber-criminal infringements: doctrine, law, and law enforcement*. Moscow: Yurlitinform. (In Russ.).

Gaudette, T., Scrivens, R., & Venkatesh, V. (2020). The role of the internet in facilitating violent extremism: insights from former right-wing extremists. *Terrorism and Political Violence*. Epub ahead of print 16 July.

Grobbelaar, A. (2022). Media and Terrorism in Africa: Al-Shabaab's Evolution from Militant Group to Media Mogul. *Insight on Africa*, *15*(1), 7–22. https://doi.org/10.1177/09750878221114375

Huddy, L., Smirnov, O., Snider, K. L. G., & Perliger, A. (2021). Anger, Anxiety, and Selective Exposure to Terrorist Violence.*Journal of Conflict Resolution*, *65*(10), 1764–1790. https://doi.org/10.1177/00220027211014937

Ishchuk, Ya. G., Pinkevich, T. V., & Smolyaninov, E. S. (2021). *Digital criminology*: tutorial. Moscow: Akademiya upravleniya MVD Rossii. (In Russ.).

Keenan, P. K. (2019). Creating spaces of public insecurity in times of terror: The implications of code/space for urban vulnerability analyses. *Environment and Planning C: Politics and Space*, *37*(1), 81–101. https://doi.org/10.1177/2399654418776660

Khokhlov, N., & Korotayev, A. (2022). Internet, Political Regime and Terrorism: A Quantitative Analysis. *Cross-Cultural Research*, *56*(4), 385–418. https://doi.org/10.1177/10693971221085343

Kraidy, M. (2018). Terror, territoriality, temporality: Hypermedia events in the age of Islamic state. *Television and New Media, 19*(2), 170–176.

Kydd, Andrew H., Walter, & Barbara F. (2006). The Strategies of Terrorism. *International Security*, *31*(1), 49–80.

Liem, M., van Buuren, J., de Roy van Zuijdewijn, J., Schönberger, H. & Bakker, E. (2018). European Lone Actor Terrorists Versus "Common" Homicide Offenders: An Empirical Analysis. *Homicide Studies*, *22*(1), 45–69. https://doi.org/10.1177/1088767917736797

Makinda, S. (2016). Terrorism in International Society: An Eclectic Perspective. *Journal of Asian Security and International Affairs*, *3*(1), 90–101. https://doi.org/10.1177/2347797015626053

Nossek, H. (2008). 'News media'-media events: Terrorist acts as media events. *Communications*, *33*(3), 313–330.

Orehek, E., & Vazeou-Nieuwenhuis, A. (2014). Understanding the Terrorist Threat: Policy Implications of a Motivational Account of Terrorism: Policy Implications of a Motivational Account of Terrorism. *Policy Insights From the Behavioral and Brain Sciences*, *1*(1), 248–255. https://doi.org/10.1177/2372732214549747

Polo, S. M. T. (2020). How Terrorism Spreads: Emulation and the Diffusion of Ethnic and Ethnoreligious Terrorism. *Journal of Conflict Resolution, 64*(10), 1916–1942. https://doi.org/10.1177/0022002720930811

Russkevich, E. A., Dmitrenko, A. P., & Kadnikov, N. G. (2022). Crisis and palingenesis (re-birth) of criminal law under digitalization. *Vestnik Sankt-Peterburgskogo universiteta*. *Pravo*, 13(3), 585–598. (In Russ.). https://doi.org/10.21638/spbu14.2022.301

Sandler, T. (2013). The analytical study of terrorism. *Journal of Peace Research, 51*(2), 257–271. https://doi.org/10.1177/0022343313491277

Schwartz, Carly. (2014, November 11). Majority of Americans Think Watching ISIS Beheadings Is Disrespectful to the Victims. *Huffpost*. https://www.huffingtonpost.com.au/entry/isis-beheading-videos_n_6194498

Shchetinina, E. V. (2018). Problems of development of the culture of violence in the Internet space. *Innovatsionnoe razvitie professionalnogo obrazovaniya*, *18*(2), 127–130. (In Russ.).

Törnberg, P., &Törnberg, A. (2022). Inside a White Power echo chamber: Why fringe digital spaces are polarizing politics. *NewMedia & Amp; Society*, 146144482211229. https://doi.org/10.1177/14614448221122915

Uusitalo, N., Valaskivi, K., & Sumiala, J. (2021). Epistemic modes in news production: How journalists manage ways of knowing in hybrid media events involving terrorist violence. *Journalism*, *23*(9), 1811–1827. https://doi.org/10.1177/14648849211015601

Zedner, L. (2021). Countering terrorism or criminalizing curiosity? The troubled history of UK responses to right-wing and other extremism. *Common Law World Review*, *50*(1), 57–75. https://doi.org/10.1177/1473779521989349

Author information

Elena Yu. Antonova – Doctor of Law, Professor, Dean of Law Faculty, Far East Juridical Institute (branch) of the University of Public Prosecution of the Russian Federation
Address: 8 Sukhanov Str., 690091 Vladivostok, Russian Federation
E-mail: antonovy@yandex.ru
ORCID ID: https://orcid.org/0000-0001-6605-3699
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/rid/ABD-6781-2021
ScopusAuthorID:https://www.scopus.com/authid/detail.uri?authorId=57205298413
Google Scholar ID: https://scholar.google.com/citations?user=dqfYMLYAAAAJ
RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=261147

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – October 24, 2022
Date of approval – December 6, 2022
Date of acceptance – March 6, 2023
Date of online placement – March 10, 2023

Научная статья
УДК 343.3/.7:004
EDN: https://elibrary.ru/hfpmtn
DOI: https://doi.org/10.21202/jdtl.2023.10

Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию

Елена Юрьевна Антонова

Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации
г. Владивосток, Российская Федерация

Ключевые слова

Вербовка,
криминализация,
право,
преступление,
пропаганда,
пространство,
противодействие,
терроризм,
финансирование,
цифровые технологии

Аннотация

Цель: выработка рекомендаций по противодействию преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

Методы: методологическую основу исследования составляют всеобщий диалектический метод познания, совокупность общенаучных и частнонаучных методов исследования, таких как анализ, синтез, логический, восхождения от абстрактного к конкретному, индукция, дедукция и др.

Результаты: определено, что развитие цифрового (кибер-) пространства и цифровых технологий способствует интенсивности терроризма, а также привело к изменению механизма совершения преступлений террористической направленности. Сделан вывод о том, что для обеспечения эффективности мер по противодействию преступлениям террористической направленности, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий, необходимы четкая стратегия и соответствующая нормативная правовая база.

Научная новизна: в работе проанализированы такие формы преступной деятельности террористических формирований, совершаемые в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, как распространение идеологии насилия и пропаганда террористической деятельности, вербовка новых членов и их обучение, применения цифровых технологий в процессе приготовительной и непосредственной террористической деятельности, финансирование.

Выявлены преимущества использования цифрового пространства и (или) цифровых технологий в процессе совершения преступлений террористической направленности. Изменение механизма совершения преступлений террористической направленности в связи с использованием цифровых технологий, по мнению автора, должно учитываться в процессе криминализации (изменении интенсивности пенализации) общественно опасных деяний. К важным направлениям государственной политики в сфере противодействия данным преступлениям отнесены воспитательно-просветительская деятельность, обучение сотрудников правоохранительных органов, расширение их полномочий для обеспечения четкого и эффективного контроля цифрового контента.

Практическая значимость: определяется возможностью использования сформулированных выводов и предложений для дальнейшей научной разработки уголовной политики государства в сфере противодействия преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

Для цитирования

Антонова, Е. Ю. (2023). Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию. *Journal of Digital Technologies and Law*, *1*(1), 251–269. https://doi.org/10.21202/jdtl.2023.10

Список литературы

Антонова, Е. Ю. (2018). Терроризм как идеология насилия. *Вестник Дальневосточного юридического института МВД России*, *2*(43), 69–74. https://elibrary.ru/usgvtk

Антонова, Е. Ю. (2022). Технологии искусственного интеллекта – субъект преступления или орудие/средство совершения преступления? *Юридический вестник Кубанского государственного университета*, *1*, 31–39. EDN: https://elibrary.ru/liybhv. DOI: https://doi.org/10.31429/20785836-14-1-31-39

Дремлюга, Р. И. (2022). *Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение*: монография. Москва: Юрлитинформ. https://elibrary.ru/hsbxrm

Ищук, Я. Г., Пинкевич, Т. В., Смольянинов, Е. С. (2021). *Цифровая криминология*: учебное пособие. Москва: Академия управления МВД России. https://elibrary.ru/vckoef

Русскевич, Е. А., Дмитренко, А. П., Кадников, Н. Г. (2022). Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации. *Вестник Санкт-Петербургского университета. Право*, *13*(3), 585–598. EDN: https://elibrary.ru/xlyjys. DOI: https://doi.org/10.21638/spbu14.2022.301

Щетинина, Е. В. (2018). Проблемы развития культуры насилия в интернет-пространстве. *Инновационное развитие профессионального образования*, *18*(2), 127–130. https://elibrary.ru/xrzrml

Dingji Maza, K., Koldaş, U., & Aksit, S. (2020). Challenges of Combating Terrorist Financing in the Lake Chad Region: A Case of Boko Haram. *SAGE Open*, *10*(2), 215824402093449. https://doi.org/10.1177/2158244020934494

Gaudette, T., Scrivens, R., & Venkatesh, V. (2020). The role of the internet in facilitating violent extremism: insights from former right-wing extremists. *Terrorism and Political Violence*. Epub ahead of print 16 July.

Grobbelaar, A. (2022). Media and Terrorism in Africa: Al-Shabaab's Evolution from Militant Group to Media Mogul. *Insight on Africa*, *15*(1), 7–22. https://doi.org/10.1177/09750878221114375

Huddy, L., Smirnov, O., Snider, K. L. G., & Perliger, A. (2021). Anger, Anxiety, and Selective Exposure to Terrorist Violence. *Journal of Conflict Resolution*, *65*(10), 1764–1790. https://doi.org/10.1177/00220027211014937

Keenan, P. K. (2019). Creating spaces of public insecurity in times of terror: The implications of code/space for urban vulnerability analyses. *Environment and Planning C: Politics and Space*, *37*(1), 81–101. https://doi.org/10.1177/2399654418776660

Khokhlov, N., & Korotayev, A. (2022). Internet, Political Regime and Terrorism: A Quantitative Analysis. *Cross-Cultural Research*, *56*(4), 385–418. https://doi.org/10.1177/10693971221085343

Liem, M., van Buuren, J., de Roy van Zuijdewijn, J., Schönberger, H., & Bakker, E. (2018). European Lone Actor Terrorists Versus "Common" Homicide Offenders: An Empirical Analysis. *Homicide Studies*, *22*(1), 45–69. https://doi.org/10.1177/1088767917736797

Makinda, S. (2016). Terrorism in International Society: An Eclectic Perspective. *Journal of Asian Security and International Affairs*, *3*(1), 90–101. DOI: https://doi.org/10.1177/2347797015626053

Orehek, E., & Vazeou-Nieuwenhuis, A. (2014). Understanding the Terrorist Threat: Policy Implications of a Motivational Account of Terrorism. *Policy Insights From the Behavioral and Brain Sciences*, *1*(1), 248–255. https://doi.org/10.1177/2372732214549747

Polo, S. M. T. (2020). How Terrorism Spreads: Emulation and the Diffusion of Ethnic and Ethnoreligious Terrorism. *Journal of Conflict Resolution*, *64*(10), 1916–1942. https://doi.org/10.1177/0022002720930811

Sandler, T. (2013). The analytical study of terrorism. *Journal of Peace Research*, *51*(2), 257–271. https://doi.org/10.1177/0022343313491277

Törnberg, P., & Törnberg, A. (2022). Inside a White Power echo chamber: Why fringe digital spaces are polarizing politics. *New Media & Amp; Society*, 146144482211229. https://doi.org/10.1177/14614448221122915

Uusitalo, N., Valaskivi, K., & Sumiala, J. (2021). Epistemic modes in news production: How journalists manage ways of knowing in hybrid media events involving terrorist violence. *Journalism*, *23*(9), 1811–1827. https://doi.org/10.1177/14648849211015601

Zedner, L. (2021). Countering terrorism or criminalizing curiosity? The troubled history of UK responses to right-wing and other extremism. *Common Law World Review*, *50*(1), 57–75. https://doi.org/10.1177/1473779521989349

Сведения об авторе

Антонова Елена Юрьевна – доктор юридических наук, профессор, декан юридического факультета, Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации
Адрес: 690091, Российская Федерация, г. Владивосток, ул. Суханова, 8
E-mail: antonovy@yandex.ru
ORCID ID: https://orcid.org/0000-0001-6605-3699
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/rid/ABD-6781-2021
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57205298413
Google Scholar ID: https://scholar.google.com/citations?user=dqfYMLYAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=261147

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 24 октября 2022 г.
Дата одобрения после рецензирования – 6 декабря 2022 г.
Дата принятия к опубликованию – 6 марта 2023 г.
Дата онлайн-размещения – 10 марта 2023 г.