FINANCIAL SECURITY

#45
MARCH/2025

Head of the Anti-Terrorist Center of the Commonwealth of Independent States

EVGENY SYSOEV:

"Effective anti-terrorist cooperation is unattainable without the unified efforts of all stakeholders engaged in combating terrorism and extremism"

YURY CHIKHANCHIN
Director of the Federal Financial Monitoring Service,
Chairman of the Editorial Board

DEAR READERS!

This year's first issue of the Financial Security Journal is dedicated to countering terrorism and terrorist financing. These threats persist as some of the most pressing challenges confronting nations today. The 2024 Global Terrorism Index published by the Institute for Economics and Peace revealed a troubling 22 % increase in terrorism-related deaths, marking the highest toll since 2017[1].

Terrorism recognizes no borders, nationality, religion, or identity. Addressing this menace requires coordinated, international action. More than 25 years ago, on December 9, 1999, the 54th session of the UN General Assembly adopted the International Convention for the Suppression of the Financing of Terrorism. Today, we reaffirm our commitment to the principles of multilateral cooperation in confronting this global threat. I would like to note that one of the Federal Financial Monitoring Service's (FFMS) key priorities is to enhance cooperation with our international partners within the framework of the United Nations, the Commonwealth of Independent States (CIS), the Collective Security Treaty Organization (CSTO), the Shanghai Cooperation Organization (SCO), BRICS, and other international platforms.

Significant progress continues within the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), the Middle East and North Africa Financial Action Task Force (MENAFATF), and other FATF-style regional bodies.

Let me note the role of the Council of Heads of Financial Intelligence Units of CIS Member States (CH FIUs), which ensures the prompt exchange of intelligence and coordinates joint actions against terrorist financing. The Council ongoing initiatives include Operation Barrier, which tracks transnational financial flows, and collaborative activities at the International Money Laundering and Terrorist Financing Risk Assessment Center (IRAC).

As terrorists use virtual assets, the development of analytical tools becomes particularly relevant. One such tool is the Transparent Blockchain digital service for monitoring cryptocurrency transactions, which is used both by the Russian AML/CFT system and international partners.

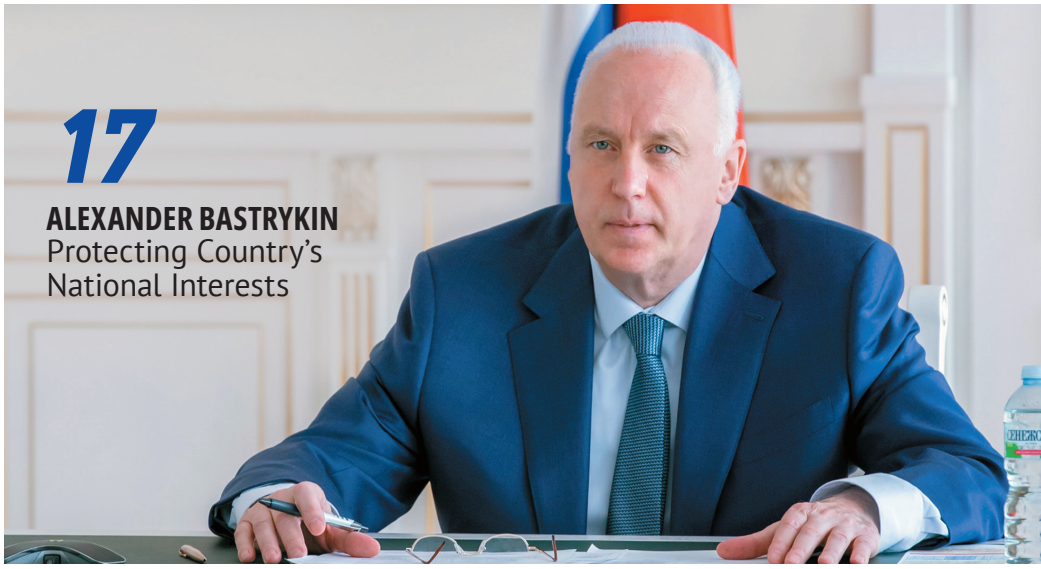
Over the years, we have successfully established a comprehensive and well-coordinated system of cooperation among law enforcement agencies, government bodies, and international organizations - laying the foundation for a robust anti-terrorism partnership.

This issue features contributions from Russian and international experts representing institutions that play an essential role in countering terrorism and terrorist financing. Topics include cyberterrorism and the misuse of advanced technologies, international cooperation to promote global security, inter-agency partnerships, and other topics.

Dear readers, I hope that the insights and expertise shared in this issue will prove valuable and offer new perspectives on the challenges we collectively explore.

[1] Key findings from the 2024 Global Terrorism Index, 29.02.2024. URL: https://www.visionofhumanity.org/7-key-findings-from-the-global-terrorism-index-2024/.

CONTENTS



Inter-Agency Partnership is Key to Long-Term Counter-Terrorism Sustainability: National Experiences

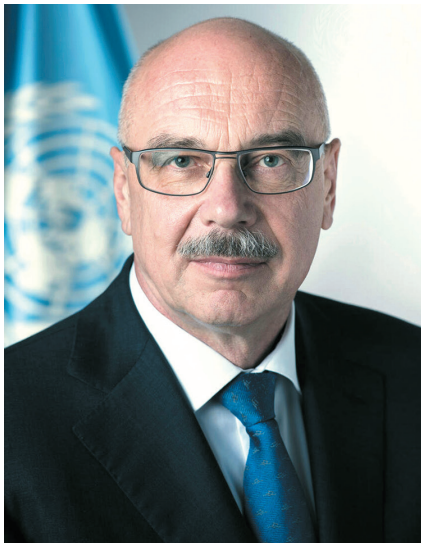
Cyber Terrorism: Emerging Challenges and Responses

Young Professionals Tribune

Anti-Money Laundering News

INTERNATIONAL COUNTER-TERRORISM EFFORTS: TOWARDS SECURE WORLD

Terrorism and the violent extremism that fuels it remain a serious threat to international peace and security, human rights, and sustainable development. These phenomena continue to inflict profound suffering on populations across the globe. A decisive and coordinated global response, particularly in combating the financing of terrorism and curbing the misuse of advanced technologies, is critical to neutralizing this threat.



VLADIMIR VORONKOV
Under-Secretary-General,
UN Office of Counter-Terrorism

Terrorist groups such as Daesh* (ISIS) and Al-Qaeda* have increasingly localized their operations, with regional affiliates gaining autonomy and becoming more decentralized. According to the 20th Report of the UN Secretary-General on the threat posed by ISIS*, conflict zones in West Africa and the Sahel have emerged as areas of particular concern. In the Middle East, Daesh* can take advantage of the security vacuum following the fall of Bashar al-Assad's Syrian government in December 2024, while detention centers and camps in northeastern Syria, housing foreign and domestic terrorist combatants remain a significant concern. For Afghanistan, the Islamic State of Iraq and the Levant – Khorasan Province (ISIS-K)* poses a significant interregional threat.

Daesh* and Al-Qaeda* continue to exploit new technologies to advance their activities, propaganda, and recruitment.
Reportedly, they are increasingly using anonymized cryptocurrencies, 3D printing, drones, and marine drones, surveillance systems and raising funds through social media using creative methods, e.g. video games and gaming platforms. They are now using AI (artificial intelligence) for propaganda and recruitment, and the darknet facilitates their cybercrime activities.

ROLE OF UNITED NATIONS AND UNOCT

The United Nations, through its counter-terrorism architecture, actively supports Member States in addressing the rising transnational threat posed by terrorism. The United Nations Office of Counter-Terrorism (UNOCT) leads the implementation of the General Assembly's counter-terrorism mandates. It also coordinates and streamlines the efforts of various UN bodies under the four pillars of the Global Counter-Terrorism Strategy. UNOCT provides targeted technical assistance and capacity-building to Member States through a broad portfolio of 18 global programs.

The Global Counter-Terrorism Strategy, adopted in 2006 by the UN General Assembly and updated biannually, provides guidance to member states on how to comprehensively address the problem of terrorism at the global level through international cooperation. The consolidation of UN counter-terrorism bodies began with the establishment of UNOCT in 2017, as the first major institutional reform under Secretary-General António Guterres.

UNOCT collaborates closely with subsidiary bodies of the Security Council. These include the Counter-Terrorism Committee and its Executive Directorate (CTED), as well as the 1267/1989/2253 ISIL (Daesh)* & Al-Qaida* Sanctions Committee, and the Monitoring Group.

COUNTERING FINANCING OF TERRORISM

Terrorist groups use both illicit and ostensibly legitimate channels to raise, store, transfer, and manage financial resources. These include donations, criminal enterprises, and commercial ventures. While conventional methods such as cash smuggling and informal value transfer systems (e.g., Hawala) remain prevalent, the use of digital platforms - social media, e-commerce, and cryptocurrencies - has grown significantly.

In response to UN Security Council Resolution 2462 (2019), UNOCT launched the Global Programme on Detecting, Preventing and Countering the Financing of Terrorism (CFT Programme). The Programme provides technical assistance to Member States at national and regional levels, and facilitates strengthening national CFT frameworks in line with the Financial Action Task Force (FATF) Recommendations.

The Programme's significant achievement was the publication of the Guidelines for the Detection, Investigation, and Seizure of the Criminal Cryptocurrencies, developed in partnership with the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) and the Federal Financial Monitoring Service (FFMS). These guidelines assist law enforcement agencies in addressing the anonymity of virtual asset platforms, decentralized finance (DeFi), non-fungible tokens (NFTs), and non-custodial wallets. The document provides actionable measures for enhancing AML/CFT compliance and enforcement. In 2025, the initiative entered its second phase, extending its application to other FATF-style regional bodies for updating and promoting the guidelines.

The EAG and UNOCT also collaborated to provide targeted support to Central Asian states. Two partners developed tailored technical assistance plans for Kyrgyzstan and Tajikistan, aimed at shielding the non-profit sector from misuse in terrorist financing.

In Eastern and Southern Africa, the CFT Programme supports regional initiatives to combat terrorist financing through the region's Anti-Money Laundering Group (ESAAMLG) and risk assessments. In the Middle East and North Africa, it has forged partnerships with entities in the United Arab Emirates, the Kingdom of Saudi Arabia, and the League of Arab States. Additionally, the Program facilitates the development of goFintel software, designed to assist financial intelligence units (FIUs) and relevant law enforcement agencies in financial investigations related to money laundering, terrorist financing, and related serious crimes.

As part of its continued development, the recently adopted Algerian Guidelines for Member States on Preventing, Detecting, and Suppressing the Use of New and Emerging Financial Technologies for Terrorist Purposes enhance the alignment of the CFT Programme with FATF Recommendations and address the technical assistance priorities identified by CTED.

The Global CFT Programme continues to reinforce risk-based approaches through regional, national, and sectoral risk assessments.

It also encompasses efforts to combat the misuse of virtual assets, protect the non-profit sector from the risk of terrorist financing, strengthen financial investigative capabilities, and leverage public-private partnerships to enhance the overall effectiveness of counter-terrorism financing measures.

>10 000
specialists worldwide

since 2020 have received training under the program, strengthening institutional capacity across the public and private sectors.

COUNTERING MISUSE OF NEW TECHNOLOGIES

Terrorist groups use advanced technologies, including 3D printing of weapon parts, AI experiments, and others, for attacks, recruitment, and financing of criminal activities.

Over the past decades, new technologies, combined with their increasing availability, have become a major driver of economic progress, but their misuse poses threat to international security and human rights. Terrorists are increasingly using the Internet and social media to radicalize, recruit, incite violence, and to claim responsibility for attacks, recruitment, fundraising, weapons procurement, and distribution of instructional materials. AI-driven systems, in particular using advanced algorithms and machine learning are also enhancing the analytical capabilities of law enforcement agencies, with relevant applications underway.

In the eighth review of the UN Global Counter-Terrorism Strategy, the General Assembly mandated UNOCT and other UN bodies to support innovative measures aimed at strengthening the capacity of states to use new technologies. Since 2021, UNOCT has trained over 4,000 officials from more than 150 countries through the Global Cybersecurity Program. The Program includes protecting critical infrastructure from terrorist cyberattacks, countering the use of the darknet by terrorists, investigation of virtual asset misuse, and digital forensics.

In October 2022, the UN Security Council Counter-Terrorism Committee unanimously adopted the Delhi Declaration outlining a unified approach to address terrorist use of emerging technologies. The elaborated recommendations will further facilitate UNOCT's work in this area.

OBSERVING HUMAN RIGHTS IN COUNTERING TERRORISM

The fight against terrorist groups included in the UN Security Council list is governed by its mandate. The United Nations Security Council and General Assembly consistently emphasize that all counter-terrorism measures must comply with international law, including international human rights law, international humanitarian law, and international refugee law.

CONCLUSION

Terrorist organizations such as Al-Qaeda* and Daesh* continue to pose a profound threat to international security, exhibiting both resilience and adaptability. Their increasing reliance on cryptocurrencies, emerging financial technologies, and anonymous digital transactions underscores the urgent need for closer international cooperation.

UNOCT, in alignment with the UN Global Counter-Terrorism Strategy and relevant Security Council resolutions, remains committed to supporting member states in countering the financing of terrorism and preventing the misuse of advanced technologies. Through its innovative programs and global partnerships, including strong cooperation with the Russian Federation, UNOCT continues to advance a unified, international response to terrorism. We value the tight and meaningful cooperation with the Russian Federation in countering terrorist threats, in particular in combating the financing of this criminal activity.

*Designated as terrorist organizations, activities are banned in the Russian Federation.

COUNTERING TERRORISM AS CORE PRIORITY OF PROSECUTION AUTHORITIES

IGOR KRASNOV
Prosecutor General of the Russian Federation,
Chairman of the Coordination Council of Prosecutors General of CIS Member States (CCPG)

In recent years, Russia has faced new threats posed by international terrorists, including the Nord Stream pipelines sabotage and the massacre at Crocus City Hall. These developments demand heightened vigilance and the unwavering commitment of all relevant agencies to confront the ideologies of terrorism, fascism, and radical religious extremism.

This issue was a focal point at the extended board meeting of the Prosecutor General's Office last year. The FFMS, as a key stakeholder, made several vital recommendations, which were incorporated into the official resolution and will serve as a foundation for a new national counter-terrorism program.

Financial intelligence agencies make a significant contribution to the overall effort to counter the financing of terrorism. Last year, prosecutors submitted to court more than 1,500 criminal cases of terrorism-related offenses, nearly equal number of extremist criminal cases, and about 200 cases related to the financing of these criminal activities.

Effective financial monitoring is instrumental in identifying and disrupting such criminal activity. The synergy between intelligence provided by FFMS and the findings of operational law enforcement work allows for timely recalibration of supervisory and enforcement efforts to suppress offences and crimes.

In 2024, law enforcement officials detected more than 200,000 violations related to countering terrorism. More than 18,000 lawsuits were initiated, almost all of them have been resolved, some are still under consideration, and 65,000 submissions were filed. This is the result of a risk-based approach and coordinated actions of the prosecution network.

The cross-border nature of terrorism requires coordination and cooperation internationally.

To achieve this, the Prosecutor General's Office has held meetings with representatives of foreign law enforcement agencies. Discussions have focused on a broad range of interconnected challenges, including combating terrorism and related problems, extremism, and illegal migration. By sharing experience with our colleagues from Cuba, Turkey, Tajikistan, Cambodia, and other countries, we have not only improved our own methodologies but also contributed to enhancing the capacity of our international counterparts.

In autumn 2024, a joint forum was convened in Belarus by the EAG and the CCPG. The forum underscored the continued importance of multilateral action in the fight against terrorism, and its outcomes clearly affirmed the value of such platforms for regional cooperation.

Finally, I would like to underscore the indispensable role of the Financial Security Journal as a professional forum for sharing insights, promoting best practices, and advancing inter-agency and international cooperation in the fields of money laundering prevention and counter-terrorism financing.

JOINING FORCES: COLLECTIVE RESPONSE TO TERRORISM

EVGENY SYSOEV:

NATIONAL SECURITY ISSUES MUST BE ADDRESSED IN CONTEXT OF INTERNATIONAL COOPERATION

Evgeny Sysoev
Head of the Anti-Terrorist Center of the Commonwealth of Independent States

This June marks the 25th anniversary of the Anti-Terrorist Center of the CIS countries (CIS ATC). Over a quarter of a century, the Center has gained extensive experience in organizing and coordinating joint counter-terrorism exercises, and has contributed to the development of more than 100 model legal acts in the field of security, in close collaboration with the CIS Interparliamentary Assembly, noted Colonel General Evgeny Sysoev, head of the CIS ATC. In an interview with Financial Security Journal, Evgeny Sysoev elaborated on why multilateral cooperation is essential for effectively countering terrorism in the Eurasian region, and highlighted the key role of Russia's financial intelligence system in advancing these efforts.

— Evgeny, this June, the CIS Anti-Terrorist Center celebrates its 25th anniversary. What results has the ATC achieved in fulfilling its regional security objectives?

— You are correct - on June 21 the ATC celebrates 25 years since its establishment. The decision to establish the ATC was taken amidst increasing terrorist and extremist activity in the post-Soviet space. The tragic impact of terrorist attacks in Kyrgyzstan, Russia, Uzbekistan, and other CIS countries underscored the urgent need for a unified counterterrorism framework and a coordinated mechanism for its implementation, tailored to the national interests of the member states.

In January 2000, following the Organization for Security and Co-operation in Europe (OSCE) Istanbul Summit in November 1999, heads of state exchanged views on international terrorism. As a result of the Summit, CIS countries' Security Councils, Council of Heads of National Security Enforcement Agencies and Special Services of the CIS, the Council of Ministers of Internal Affairs, and the Council of Ministers of Defense were instructed to develop a targeted program to combat international terrorism and extremism. These instructions also included the establishment of a common anti-terrorist center. Six months later, on June 21 in Moscow, the meeting of the CIS Heads of State made a number of decisions, including on the establishment of the Anti-Terrorist Center.

I should mention that, due to the heightened terrorist threat globally, other international organizations followed suit in establishing coordinating counter-terrorism bodies. For example, in June 2002, the Shanghai Cooperation Organization signed the Agreement on the Regional Anti-Terrorist Structure (RATS), now a permanent body of the SCO.

Speaking about the results achieved over the years of the CIS ATC work, I must note, first of all, coordinated joint measures of competent authorities in CIS countries in locating and apprehending individuals involved in terrorism and extremism who were attempting to evade justice. Thanks to an established and efficient mechanism for information exchange, and in cooperation with security agencies in both CIS and CSTO member states, nearly 800 wanted persons have been apprehended over the past decade based on the ATC-supplied intelligence.

CIS ATC Specialized Data Bank plays a crucial role in this process. It provides real-time access to information for CIS members' competent authorities and contains thematic datasets on more than 17,000 individuals wanted for terrorism, extremism, or mercenary activity, as well as an image archive of over 12,500 photographs.

Secondly, I must emphasize that these achievements were made possible due to an established and evolving organizational and legal framework. For instance, in 2005 the Council of Heads of State adopted the Concept of the CIS Member States Cooperation in Combating Terrorism and Other Violent Forms of Extremism. In 2007, the Treaty on combating money laundering and countering the financing of terrorism was signed. Anti-Terrorist Center was involved in developing a number of important documents, including the Agreement on the protection of classified information in CIS (2013) and the Agreement on information exchange in CIS for countering terrorism and other violent forms of extremism and their financing (2017).

Of particular significance is our collaboration with the Inter-Parliamentary Assembly of the CIS, which has yielded over 100 model legal acts aimed at harmonizing national security legislation across member states.

The Center is also the principal architect behind the medium-term interstate cooperation programs on countering terrorism and extremism within the CIS. This year, the Council of Heads of State will consider the tenth such program.

Thirdly, the Center provides assistance in organizing advanced training for counter-terrorism officers. To date, more than 2,000 officers from the counterterrorism divisions of CIS national security agencies and special services have completed advanced training through programs developed and facilitated by the ATC.

« The tragic impact of terrorist attacks in Kyrgyzstan, Russia, Uzbekistan, and other CIS countries underscored the urgent need for a unified counterterrorism framework and a coordinated mechanism for its implementation, tailored to the national interests of the member states.

Fourthly, over a quarter of a century, the Center has gained extensive experience in organizing and conducting joint counterterrorism exercises. Since its inception, the ATC has coordinated 20 such drills across CIS countries, significantly enhancing the operational coherence and readiness of competent authorities to prevent and stop terrorist acts.

Fifthly, the ATC also serves as a key platform for dialogue, information exchange, and strategic alignment. This includes regular meetings of the heads of national counterterrorism centers, regional expert consultations, and plenary sessions chaired by the ATC and attended by plenipotentiary representatives from all member states. Since 2023, we launched a new initiative, the CIS Conference on Countering Terrorism and Extremism – which broadened the scope of regional and international engagement.

That said, despite our accomplishments, we must remain vigilant. No system, no matter how advanced, can offer absolute protection against terrorism. Underestimating potential and actual terrorist threats can lead to tragic consequences.

— How would you characterize the role of international cooperation in this effort? What current trends have you observed?

Effective anti-terrorist cooperation is unattainable without the unified efforts of all stakeholders engaged in combating terrorism and extremism. Chief among them are the competent authorities whose leaders convene semiannually under the CIS framework. The ATC maintains strong ties with key regional bodies, including: the Council of Commanders of Border Troops and its Coordination Service, the Council of Ministers of Defense and its Secretariat, Council of Ministers of Internal Affairs and the Office for the Coordination of the Fight Against Organized Crime and Other Dangerous Types of Crime in CIS member states, Coordination Council of Prosecutors General, Council of Heads of Penitentiary Services, Council of Heads of Migration Authorities, Council of Heads of Customs and its Committee comprised of heads of law enforcement departments, Transport Coordination Session, Coordination Council of Heads of Tax (Financial) Investigation Bodies. I would like to emphasize the cooperation with the Council of Heads of Financial Intelligence Units. This network allows us to pool capabilities, unify resources, and significantly improve the effectiveness of counter-terrorism measures.

The Center has also developed and documented relations with relevant international and regional organizations mandated to counter terrorism, most notably the CSTO and SCO, which, as President Vladimir Putin noted, are the CIS's "natural partners". In addition, we engage with UN counter-terrorism bodies, INTERPOL, EAG, OSCE, and Central Asian Regional Information and Coordination Center (CARICC).

Speaking of current trends in international cooperation, one should note that it is aimed at enhancing the role of regional organizations in global efforts to counter terrorism and extremism. Organizations such as the ATC CIS and the Regional Anti-Terrorist Structure of the Shanghai Cooperation Organization (SCO RATS) are not only active participants in actions of the leading international organizations but also contribute significantly to the analytical reports prepared by the Monitoring Group of the UNSC Sanctions Committees on ISIS* and Al-Qaeda*, and to the UNSC Counter-Terrorism Committee on the results of country missions and monitoring of the implementation of relevant UNSC resolutions.

However, the increasing politicization of international cooperation in countering terrorism and extremism has had a detrimental effect. This resulted in the dissolution of a number of forums, such as the OSCE Counter-Terrorism Conference. Western states attempt to force

> **The Center established platforms for exchanging information and best practices, aligning efforts, and discussing further work.**

Russia out of international structures (e.g. the country's FATF membership has been suspended), despite the fact that terrorists and extremists benefit from such counter-productive measures.

— What are key factors influencing the emergence and development of terrorist threats in the post-Soviet space?

— We believe that the main drivers stem from instability in neighboring regions - particularly Syria, Iraq, Palestine, Israel, Afghanistan, Pakistan.

Security threats to CIS countries originating from the Afghanistan and Pakistan region are caused by the political turbulence in Afghanistan, the persistent level of combat potential of terrorist organizations in the country, and the increasing recruitment activity in the Central Asia. Primarily, the Islamic State – Khorasan Province*.

The conflict in the Gaza Strip has triggered an increase in terrorist activity in a number of CIS countries. There were incidents of destabilization fueled by pro-Palestinian demonstrations, rising anti-Semitic sentiments, and participation of nationals from Central Asia and Russia in combat operations on behalf of Hamas. We hope that a durable ceasefire will contribute to stability both in the Middle East and in the CIS region.

— How serious is the threat of cyberterrorism and technological misuse by terrorists?

— The threat is increasingly severe. These concerns are regularly discussed at international expert meetings.

In December, for example, we hosted representatives from the Monitoring Group of the UNSC Sanctions Committees in the run-up to their preparation of the latest report on ISIS*. In particular, we noted growing trends in the use of virtual preachers and self-learning bots by terrorist groups to recruit followers and disseminate radical ideology. In the context of countering the financing of terrorism, particularly challenging becomes the use of new information technologies, e.g. cryptocurrencies and anonymizers, to obscure terrorist support activities.

In this regard, the development of cyber offensive strategies should thus be a priority for international cooperation. Competent authorities must be equipped with the necessary powers and advanced tools to not only identify potential terrorist groups online but also to proactively disrupt recruitment efforts, financial flows, and logistical support channels used by terrorist organizations.

With the rise of modern communication technologies, regional and national initiatives, as well as special programs promoting cooperation in countering terrorism and extremism, demonstrate the greatest practical potential.

We place high expectations on the UN Convention against Cybercrime, adopted by UN General Assembly Resolution 79/243 on December 24, 2024. Additionally, much is anticipated from the strengthening of international cooperation in combating certain crimes committed through information and communications systems and in the exchange of electronic evidence relating to serious crimes. This will provide a framework for the just regulation of the digital environment in the interest of the entire international community.

Therefore, key issues of ensuring national and common security must be addressed in the context of international cooperation.

— Is cooperation with national financial intelligence services effective?

— I would break it up: cooperation in the CIS countries, i.e. with the CH FIUs[1], and a broader work in the EAG[2]. In 2014, we signed cooperation agreements with both.

As for the CH FIUs, our cooperation is the most effective during the international Operation Barrier, as the ATC provides information support by regularly updating information on persons wanted for terrorist offenses. We recently reviewed the

[1] Council of Heads of Financial Intelligence Units of CIS Member States.
[2] The Eurasian Group on Combating Money Laundering and Financing of Terrorism.

results of our cooperation: since 2015, 870 persons involved in terrorist financing have been identified based on the information provided by the Anti-Terrorist Center.

In 2024, through cooperation with CH FIUs, we expanded the scenario for joint counter-terrorism training. Information exchange between the competent authorities participating in the training was supplemented with data from the Money Laundering and Terrorist Financing National Risk Assessment Center. Cryptocurrency transactions of terrorist accomplices were monitored using the Transparent Blockchain service. In my opinion, considering the relevance of the use of cryptocurrency in illicit activities, including terrorism and extremism, this area of cooperation with financial intelligence holds great promise.

The CIS ATC and the EAG have developed constructive cooperation. One of the important outcomes of this joint work has been the typological studies that identified threats specific to our common space. These studies enabled the profiling of an international terrorist fighter and recruiter; in addition, a vulnerability related to the lack of control over airline ticket purchases for terrorists has been uncovered.

We acknowledge the secretariats of the CH FIUs, the EAG as well as the ITMCFM[3] for support in organizing and conducting seminars for representatives of financial intelligence units and special services. These efforts not only enhance the competence of personnel but also provide a platform for sharing experiences in conducting investigations into the financing of terrorism. We hope that this beneficial practice will continue to develop in the interests of our countries' security.

— What is the degree of threat posed by the recruitment of young people for terrorist and extremist activities in CIS member states? Are there preventive measures in place?

— One of the priorities of CIS activities, as stated in the Concept for the Further Development of the Commonwealth of Independent States adopted in 2020, is to counter the ideology and propaganda of terrorism and to prevent the recruitment of civilians by terrorist and extremist organizations.

Young people and minors are among the main targets of propaganda and agitation of terrorism ideologists who seek to expand their number of followers and accomplices.

An analysis of the current situation in countering terrorism and extremism indicates a trend of increased involvement of minors and young people in terrorist activities. This negative trend is confirmed by our partners in the CIS countries.

Radicalization leading to terrorism, separatism, and extremism has become a global problem. The spread of radical ideologies, religious intolerance, ethnic and racial discrimination, ideas of fascism and chauvinism by terrorist groups and their sponsors, including online, is especially harmful to the minds and worldviews of young people.

The focus of terrorists on recruiting young people is due to the specific psychology of this age group – namely, an immature worldview, which makes youth more susceptible to outside influences because of their limited life experience, heightened sense of justice, and maximalist thinking.

The issue of religious deradicalization, especially when individuals subjected to targeted manipulation adopt radical Islamist ideologies, is currently more relevant in Central Asian states and Russia, and is almost nonexistent in Belarus and Moldova.

«Security threats to CIS countries originating from the Afghanistan and Pakistan area are driven by the ongoing political instability in Afghanistan, the sustained combat capabilities of terrorist organizations operating in the country, and the escalating recruitment efforts targeting Central Asia.

[3] International Training and Methodology Center for Financial Monitoring.

In September 2024, the CIS basic research organization for problems of countering terrorism and other forms of extremism (Research Center of the Federal Security Service of Russia), along with experts of the CIS ATC developed Guidelines for improving the system of measures to counter youth radicalization in CIS member states. The document was approved at the 55th meeting of the Council of Heads of National Security Enforcement Agencies and Special Services of the CIS.

Propaganda by moderators of terrorist and extremist content, disseminated through information and communication technologies, has prompted the CIS to develop an effective deradicalization program. This program is primarily aimed at preventing the development and spread of terrorist and extremist views and beliefs among minors and young people.

Initiated by President Shavkat Mirziyoyev of Uzbekistan, a draft of this program was prepared in 2022. Key developers later included the State Security Service of Uzbekistan, Research Center of the Federal Security Service of Russia, and the CIS ATC.

The Council of Heads of States approved the Program of CIS States Cooperation in Deradicalization for 2025-2027 on October 8, 2024.

In 2023, the Anti-Terrorist Center prepared an informational and analytical report on the activities of competent authorities in CIS countries related to preventing terrorist and extremist crimes among minors and young people. The report presents the practical experiences of competent authorities in this area and offers recommendations for improving preventive efforts among minors and youth.

I would like to add that since 2021, the Anti-Terrorist Center, together with the Moscow State Linguistic University (the basic organization for languages and culture of the CIS member states) has been holding an annual international contest entitled "Student Shield." It is aimed at fostering resistance to terrorist and extremist ideology among youth and supporting the best student-led initiatives in this area across CIS countries. We have observed a steady increase in interest in this event: last year, 289 students from 33 universities across 11 countries submitted their papero.

— What are ATC's short-term and long-term tasks?

— First of all, our efforts will focus on implementing the measures outlined in the Program of Cooperation in Countering Terrorism and Extremism for 2026-2028, as well as in the above-mentioned Program of Cooperation in Deradicalization for 2025-2027.

Given that effective cooperative counter-terrorism efforts largely depend on the level of international engagement, we will continue to work to involve as many interested partners as possible and to develop new forms of cooperation. A notable initiative for the CIS was the holding of an annual conference on countering terrorism and extremism, first held in Kyrgyzstan in 2023. The following year, the conference was expanded and held jointly with the SCO RATS scientific-practical conference on the same topic. This year, we plan to invite other international organizations to co-host the forum.

In addition, we also continuously work to enhance the content of our joint counter-terrorism training exercises. The ATC has previously integrated a military component into these exercises, involving the ministries of defense of CIS countries. This year, we plan to unite the potential of the CIS and CSTO into a single conceptual framework.

Furthermore, we look forward to continued cooperation with the CIS financial intelligence units, represented by the CH FIUs, both in training and in practical operations aimed at identifying individuals and channels involved in terrorist financing. I believe this area holds strong potential.

* Designated as terrorist organizations, activities are banned in the Russian Federation.

Alexander Bastrykin

Chairman of the Investigative Committee of the Russian Federation, Professor, Honored Lawyer of Russia, Doctor of Law

ALEXANDER BASTRYKIN: PROTECTING COUNTRY'S NATIONAL INTERESTS

Amid the growth of international organized crime, the increased cross-border movement of funds resulting from evolving economic relations, and the expansion of cyberspace, the effectiveness of the anti-money laundering and countering the financing of terrorism (AML/CFT) system is especially important within the broader framework of national security measures in the Russian Federation[1].

In response to urgent threats, the Investigative Committee of the Russian Federation works closely with the Federal Financial Monitoring Service (FFMS), the Bank of Russia and credit institutions, the Federal Tax Service of Russia, the Federal Security Service of Russia, and the Ministry of Internal Affairs of Russia. These well-coordinated joint efforts have resulted in the efficient detection of complex, latent crimes.

[1] Decree of the Russian Federation President dd. Feb. 07, 2021 No. 400 On the National Security Strategy of the Russian Federation. Corpus of Legislation of the Russian Federation, No. 27 (Part II), Art. 5351 dd. May 07, 2021.

> 2.5 thousand criminal cases of terrorism-related offenses (+78%)

were processed by the investigative bodies of the Investigative Committee in 2024, including 166 cases of offenses related to the financing of terrorism (115 in 2023). By the end of the year, 429 criminal cases were submitted to court (299 in 2023); including 50 cases related to terrorism financing (38 in 2023).

Courts received 796 criminal cases involving extremist acts - an increase of one-third compared to 2023. The number of individuals charged with financing extremist activities also rose, from 27 to 44.

It should be emphasized that under current circumstances inter-agency cooperation and the prompt suppression of terrorist, extremist, and other destructive activities are of particular importance.

As noted at the National Anti-Terrorism Committee meeting on February 11, 2025, coordinated efforts by law enforcement agencies prevented 23 terrorist attacks since the beginning of the year. A significant portion of these plots was orchestrated under the direction of managers and recruiters from international terrorist organizations[2].

In investigating terrorism and extremism cases, investigators thoroughly examine the circumstances of persons getting involved in illegal activities, pathways and means of radicalizing them, as well as sources and channels of financing these activities.

At the same time, curbing terrorist threats remains a global challenge that requires collective international action of different countries. BRICS has undertaken practical steps in this regard.

At the 16th BRICS Summit in Kazan in October 2024, member countries adopted a declaration emphasizing the need for deeper cooperation in counter-terrorism and disrupting terrorism financing[3].

BRICS reaffirmed its commitment to preventing and combating illicit financial flows, money laundering, terrorism financing, and the use of new technologies, including cryptocurrencies, for criminal and terrorist purposes.

One of the possible ways of cooperation appears to be joint monitoring of extremist and terrorist content on the Internet.

Advances in information and communication technology and its accessibility have enabled terrorist and extremist groups to exploit the Internet and social media for committing a wide range of offences, including incitement, radicalization, recruitment, training, and financing of terrorism and extremism.

Ongoing upgrade of AI, robotics, biotechnology, self-driving cars and drones - pose further risks of their utilization in a broader range of criminal activities.

The rise of digital innovation in data processing has created a hyper-connected world in which information is exchanged almost instantaneously.

This requires reshaping law enforcement operations. Investigators must adapt their methods of detecting, seizing, and documenting digital evidence to meet new technological realities.

Modern data analysis technologies, including artificial intelligence, facilitate the processing of vast data sets, the identification of patterns, threat detection, and preemptive response.

Though relatively new in law enforcement, these technologies are actively employed by Investigative Committee officers during preliminary investigations, contributing significantly to crime-solving outcomes.

The following key areas of AI application in crime investigations include:

- detection and analysis of digital and other forensic traces in cybercrime investigations;
- development of forensic techniques for detecting, preserving, and recovering digital traces;
- enhancement of the quality of digitally recorded evidence;
- evaluation of evidentiary credibility;
- developing decision-making support systems (e.g., suspect profiling) and automating technical operations in investigative activities (e.g., voice-to-text transcription);
- analysis of large data sets (e.g., phone records, biometric databases).

Judicial and investigative materials reveal that terrorist and extremist collaborators use digital payment methods, such as e-wallets, to

[2] The Director of the Federal Security Service of Russia Holds the National Anti-Terrorism Committee Meeting in Moscow. http://nac.gov.ru/nak-prinimaet-resheniya/direktor-fsb-rossii-provyol-v-moskve-zasedanie-0.html.
[3] Kazan Declaration - Strengthening Multilateralism For Just Global Development And Security (adopted in Kazan on 10/23/2024). Russian President's official website http://kremlin.ru/.

conceal transactions. They also establish websites and online stores distributing extremist and terrorist materials to raise funds.

For example, in 2024, a court in Ingushetia convicted two persons who had raised about 30 million rubles on one of the social networks banned in the Russian Federation, and transferred the money to an ISIS* member.

In another case, a Russian citizen organized a "charitable" fundraiser in Kazan, collecting 152,000 rubles from like-minded individuals, which he sent to ISIS* members.

In 2024, two members of an organized criminal group were convicted for drug trafficking through an online store in Buryatia during 2022-2023. To disguise the origin of their illicit funds, the offenders made a series of transactions converting money into cryptocurrency and back into fiat currency.

The existing practice shows that amidst the general digitalization of various industries and availability and prevalence of virtual banking instruments, one of the most urgent tasks is the timely detection of transactions involving transfer of assets for financing illegal activity.

There remain significant risks of financing terrorism and extremism through information and communication technologies, particularly in connection with the use of digital assets. The absence of a clear legislative framework for handling crypto-assets hampers investigative procedures and complicates seizure efforts.

"Investigative Committee officers continue to use available advanced technologies in preliminary investigations, enhancing the effectiveness and efficiency of their work.

The abundance of foreign cryptocurrency exchanges and their operation across multiple jurisdictions increases the risks of using virtual assets to conceal illicit activity.

In this connection, the Investigative Committee proposed amendments to the Criminal Code and the Rules of Criminal Procedure to recognize digital currency as an asset, to define procedures for its confiscation, to classify it as material evidence, and regulate its seizure during criminal investigations.

One must understand that terrorism and extremism are often linked to other crimes, such as money laundering and the use of criminal proceeds to finance terrorist activity.

Despite the inherent challenges of evidence collection, the Investigative Committee has achieved demonstrably positive results in detecting and investigating such crimes.

In 2024, reports of money laundering crimes rose from 242 to 280 (+15.7%).

Investigators initiated 202 cases (146 in 2023, +38%), with 72 submitted to court (65 in 2023, +11%).

Without a doubt, the cooperation framework with the Federal Security Service of Russia, the Ministry of Internal Affairs of Russia, the Federal Financial Monitoring Service, the Federal Tax Service of Russia, and others largely contributed to this result.

A notable example is the prosecution of five members of a criminal network who defrauded citizens in the Penza Region through Ponzi schemes, stealing over 2.8 billion rubles. The laundered proceeds were funneled through affiliated companies and used to purchase real estate, among other methods.

To conclude, prevention lies at the heart of the fight against terrorism and extremism.

The websites of the Investigative Committee and regional investigative bodies publish daily updates on the progress and results of the detection and investigation of terrorism- and extremism-related crimes.

The media play a crucial role in promoting zero tolerance for extremist and terrorist ideologies. By engaging experts in fields such as history, sociology, political science, and journalism, the media can support society's broader efforts to counter these threats.

This work in the information space is vital and must be actively supported and encouraged.

* Designated as terrorist organizations, activities are banned in the Russian Federation.

TERRORIST FINANCING AS GLOBAL THREAT

According to the UN General Assembly resolution, the financing of terrorism is a matter of grave concern to the international community, as the scale and severity of terrorist acts are directly influenced by the financial resources available to perpetrators[1]. For this reason, global efforts to prevent and suppress terrorist financing must be regarded as a fundamental pillar in the broader fight against terrorism.

IVAN KORNEV
Deputy Director of the Federal Financial Monitoring Service

Combating terrorist financing requires a unified effort between the private financial sector and public authorities, including law enforcement, regulatory, supervisory, and other competent agencies.

A joint assessment conducted in the Eurasian region in 2022 identified the following terrorist financing risks:

- Fundraising via the Internet;
- Collection and transfer of funds from family members to terrorists for basic needs;
- Use of bank accounts and cards;
- Smuggling of cash;
- Transfers made without opening bank accounts (e.g., through money transfer systems and electronic payment services);
- Potential misuse of funds for purchasing airline tickets for foreign terrorist fighters.

One of the current trends is the use of virtual platforms by terrorists to both raise and move funds. Criminals have developed advanced methods for anonymizing financial flows, including the use of spoofed phone numbers, multiple bank accounts, e-wallets registered under false identities, and other deceptive practices. Crowdfunding platforms intended for legitimate purposes are increasingly being exploited for illicit fundraising.

Virtual assets (cryptocurrencies) are also increasingly being used to finance terrorism. Whereas a few years ago, the United Nations estimated that fewer than 5% of terrorist attacks were financed using cryptocurrencies. That figure has since risen to 20%, or one in every five terrorist attacks[2].

Still, the so-called traditional sources of financing terrorism from the proceeds of other crimes remain relevant. These include: drug trafficking and distribution; illicit trade in arms and ammunition, oil products, cultural heritage; piracy; robbery; fraud; extortion

[1] Preamble to the International Convention for the Suppression of the Financing of Terrorism (adopted by UN General Assembly resolution 54/109 of December 9, 1999).

[2] UN Says Crypto Use in Terror Financing Likely Soaring. URL: https://www.bloomberg.com/news/articles/2022-10-31/un-finding-more-cases-where-crypto-involved-in-terror-financing.

and kidnapping; provision of illegal migration services. We also note that international terrorist organizations continue to exploit legitimate investments in commercial enterprises across the EU, Middle East, Africa, and South-East Asia.

All of the above methods enable terrorists to raise and transfer funds, often across borders, which poses risks at the supranational level. Consequently, countermeasures must be developed and implemented on a transnational scale.

An effective response to terrorist financing is impossible without efficient international information exchange, the implementation of criminal prosecution measures, and other forms of cooperation among states. While the development of bilateral or multilateral partnerships among competent authorities is essential, it is insufficient on its own; a comprehensive approach to organizing international cooperation is required.

A key international actor in this field is the Financial Action Task Force (FATF). The FATF's 40 Recommendations[3] have laid the foundation for a unified global strategy to combat money laundering, terrorist financing, and proliferation financing, maintaining system integrity at an acceptable level.

As the principal developer of global AML/CFT standards, the FATF consolidates national practices and research, enabling the adoption of the most effective strategies.

For example, the rising influence of neo-Nazism has been observed in recent years. The global environment demonstrates the importance of monitoring to prevent the escalation of this problem.

In 2021, the FATF published a study on the financing of ethnically or racially motivated terrorism[4]. In 2023, it released a report on terrorist crowdfunding, reflecting the experiences of various countries in addressing this issue[5]. These efforts help member states stay informed of evolving terrorist financing risks and implement timely countermeasures.

Obviously, a country's preparedness for international cooperation depends on the level of the national CFT framework.

The Russian Federation has an effective national system for countering the financing of terrorism, which enables it to timely take organizational, coordination, analytical, operational, and regulatory measures. The FATF has highly appreciated the country's inter-agency cooperation in investigating criminal cases of terrorist financing.

The Federal Financial Monitoring Service together with law enforcement agencies take part in various studies initiated on international platforms, as well as represent a unified and coordinated

[3] International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation // URL: fedsfm.ru/content/files/documents/2018/рекомендации%20фатф.pdf.

[4] Ethnically or Racially Motivated Terrorism Financing // URL: www.fatf-gafi.org/publications/methodandtrends/documents/ethnically-racially-motivated-terrorism-financing.html.

[5] Crowdfunding for Terrorism Financing October 2023. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf.

approach in the meetings of the FATF-style regional body (Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)), a number of other international structures, and thematic events and projects held under the auspices of the United Nations.

EAG platforms promotes researches aimed at enhancing the regional anti-money laundering infrastructure. In 2023, methodological guidelines were updated to include procedures for adding or removing individuals from terrorist and extremist lists, as well as for freezing (seizing) their assets. Ongoing efforts include the development of a bulletin on the activities of terrorist groups in Eurasia, intended to raise awareness of the methods and resources terrorists use to finance their operations.

One of the most prominent platforms in the Commonwealth of Independent States in this area is the Council of Heads of Financial Intelligence Units of the CIS Member States (Council or CH FIUs), where I serve as the head of the Secretariat.

As part of its counter-terrorist efforts, CIS countries regularly exchange information on the current CFT situation, develop joint project plans, review and consolidate input from member states, etc.

The working group on countering the financing of terrorism (WGCFT) fulfills the tasks and functions assigned to CH FIUs in the area of countering terrorist financing. It identifies priority cooperation areas, oversees the preparation and execution of coordinated CFT measures, and facilitates the exchange of operational and financial intelligence. The WGCFT also implements joint practical CFT measures.

« The FATF's role as the primary developer of global AML/CFT standards enables it to consolidate and promote application of best practices and research outcomes from various jurisdictions.

Another key initiative of the Council is the establishment of the International Money Laundering and Terrorist Financing Risk Assessment Center (IRAC), created under an agreement signed by CIS heads of state in August 2024. IRAC currently holds records on more than 40,000 individuals and legal entities linked to terrorism, Ponzi schemes, drug trafficking, and other criminal activity.

The WGCFT regularly conducts Operation Barrier, a recurring effort by the CH FIUs to identify individuals involved in international terrorist organizations, their financing networks, and ideological centers.

An essential component of any CFT framework is the freezing of assets of persons involved in such activities. In global practice, terrorist financing is countered through the application of targeted financial sanctions. Under UN Security Council Resolution 1373 (2001) and FATF Recommendation 6, all countries are required to impose such measures to prevent and suppress terrorism and its financing.

Based on the Follow-up Report on Russia's AML/CFT/CPF system, approved at the EAG Plenary Meeting in December 2023, the mechanism established in Russia for immediate freezing of assets linked to persons and entities listed under UN Security Council sanctions received a favorable review. The implementation timeframe for applying targeted financial sanctions currently does not exceed 24 hours.

In conclusion, I would like to stress that we believe it necessary to further expand international cooperation among financial intelligence units in countering the financing of terrorism. Only through collaborative efforts can we mitigate the risks of financial and material support of terrorist activities.

INTERNATIONAL COOPERATION FOR GLOBAL SECURITY

MEASURES TAKEN BY REGIONAL ANTI-TERRORIST STRUCTURE OF SHANGHAI COOPERATION ORGANIZATION TO COUNTER FINANCING OF TERRORISM

Since its establishment on June 15, 2001, the Shanghai Cooperation Organization (SCO) has become one of the most reputable and dynamic international structures, currently uniting 10 states. In 2023-2024, the Islamic Republic of Iran and the Republic of Belarus joined the Shanghai family. Today, SCO covers one-third of the globe (1,855,790 km^2) with a combined population of over 3.5 billion people.

ULARBEK SHARSHEEV
Director of the Executive Committee of the Regional Anti-Terrorist Structure (RATS) of the Shanghai Cooperation Organization

The organization is not a military unit and does not seek political dominance. Its core priorities include preserving stability and security, jointly countering terrorism, separatism, and extremism in all their forms, supporting the sustainable development of its member states, and improving the well-being of their populations. The organization's permanent bodies are located in Beijing (SCO Secretariat) and Tashkent (RATS Executive Committee).

SCO member states have clearly defined the concept of terrorism in the organization's foundational documents. The common understanding has laid the groundwork for the development of a framework of counter-terrorism measures, thereby enhancing collaboration among competent authorities and bolstering the counter-terrorism capacity of each member state of the SCO.

Terrorism stems from unresolved social, economic, and political problems, compounded by interreligious and interethnic contradictions. External interference that hinders the establishment of a multipolar world further exacerbates these conditions and fosters radicalization. International terrorist organizations are frequently exploited as instruments to destabilize certain regions and serve geopolitical interests.

Counter-terrorism cannot be effective if it is limited to reactive measures. Terrorist organizations cannot operate without consistent financial support and access to resources. These resources are required for acquiring weapons, explosives, ammunition, forged documents, and recruiting supporters. To obtain funding, terrorists often collaborate with foreign intelligence services and organized crime groups or profit from illicit activities, including drug trafficking.

Rapid advancements in technology have transformed daily life and introduced new means of payment and opportunities for terrorist financing. Cryptocurrencies, crowdfunding, and various methods of raising and transferring money via the Internet have become commonplace. The use of artificial intelligence by terrorist actors now poses a significant threat.

These new challenges and threats require closer cooperation among competent authorities in SCO member states and stronger engagement with international institutions.

In accordance with the SCO's foundational documents and related regulations[1], countering the financing of terrorism remains a key focus of cooperation among member states. Due to the measures taken, including enhanced information exchange, 101 terrorist financing channels have been identified in SCO states over the past two years.

The need for broader engagement and enhanced cooperation in countering terrorism financing has been incorporated into the Program of Cooperation of SCO Member States in Countering Terrorism, Separatism, and Extremism for 2025-2027, which was adopted by the SCO Council of Heads of States on July 4, 2024.

« SCO RATS remains open to dialogue, consolidation of efforts, and cooperation in this area with relevant international organizations and anti-terrorist structures of all interested parties.

To intensify efforts against the financing of these three threats, the Rules of Procedure for the Universal Group of Experts have been amended to include a new function - allowing the participation of Financial Intelligence Units (FIUs) representatives in SCO RATS activities as part of national delegations. Experts from the Federal Financial Monitoring Service of Russia were the first to respond and are now actively involved in organizing these meetings. It is expected that other SCO member states' financial intelligence agencies will follow this positive example.

An effective system requires clear algorithms and coordinated measures that define the roles and interactions of security services, law enforcement agencies, national financial intelligence units, and international structures. Experts from the competent authorities, with the support of the RATS Executive Committee, are currently working to establish such mechanisms.

One of the RATS Executive Committee's priorities is fostering cooperation with profile international structures. For instance, it has collaborated successfully with the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) for over 20 years. The shared membership between the two organizations facilitates efficient exchanges of information, analytical materials, regulatory frameworks, and participation in joint events.

To further strengthen this cooperation, SCO RATS and EAG are considering the development of a joint Action Plan. A common understanding of the need to intensify joint efforts and continue coordinated work was confirmed during a bilateral meeting of the delegations held in Indore, India.

Let me emphasize that SCO RATS remains open to dialogue, consolidation of efforts, and cooperation in this area with relevant international organizations and anti-terrorist structures of all interested parties.

[1] Charter of the SCO, Shanghai Convention on Combating Terrorism, Separatism, and Extremism, SCO Convention against Terrorism, SCO RATS Agreement, Concept of Cooperation of SCO Member States in Combating Terrorism, Separatism, and Extremism.

BRICS COUNTER-TERRORISM WORKING GROUP: STRENGTHENING COLLECTIVE SECURITY

Russia's presidency of BRICS in 2024 marked a significant milestone in the advancement of counter-terrorism cooperation within the association. With the accession of new members, including Indonesia, the scope of cooperation has expanded significantly, allowing for a more effective dialogue on current threats posed by international terrorist organizations and the development of timely recommendations on measures to address these threats.

SERGEY VERSHININ
Deputy Minister of Foreign Affairs of the Russian Federation

The BRICS Counter-Terrorism Working Group (CTWG) was established in 2013 when senior security officials from the BRICS states met in Cape Town, South Africa and agreed to create a dedicated platform for discussing a wide range of counter-terrorism security issues. This decision was driven by growing concerns about global security threats posed by terrorism. Member states agreed to work together to develop tools to tackle these threats. In particular, we focused on disrupting the cross-border mobility of foreign terrorist fighters (FTFs), preventing the spread of extremist ideology, and disrupting channels and sources of financial support for terrorists.

The group also prioritized intensifying information sharing, improving mechanisms for mutual legal assistance in relevant criminal investigations, and coordinating positions in international organizations - most notably, the United Nations.

It is important to note that discussions with the CTWG are conducted in a strictly professional manner. The fundamental principles guiding BRICS cooperation in this domain include respect for the sovereignty of member states and non-interference in internal affairs; adherence to international law and recognition of the United Nations' central role in maintaining peace and security; a policy of zero tolerance toward government support for terrorism; the rejection of double standards in counter-terrorism and counter-extremism efforts; and consensus-based decision-making.

A significant milestone was the adoption of the CTWG Position Paper at the 9th Plenary Session of the CTWG (Moscow, July 22–24, 2024), held under Russia's chairmanship. This document reaffirms BRICS' commitment to the Anti-Terrorism Strategy and the related Action Plan. It also outlines CTWG's future role within the global counter-terrorism architecture, offers recommendations for future work, and underscores the need for coordinated action in multilateral platforms, particularly the United Nations.

Since the Group's establishment, BRICS countries have succeeded in developing a comprehensive set of foundational documents. In particular, the 2018 South African Chairmanship approved the CTWG Rules of Procedure. In 2020, at Russia's initiative, the BRICS Anti-Terrorism Strategy was adopted; followed in 2021 by India's adoption of the Action Plan for implementing the Strategy.

The CTWG has been evolving over the last few years. There are five subgroups of experts in different areas, launched in 2020: Countering Foreign Terrorist Fighters (co-chaired by Russia and I.R.Iran), Deradicalization (China and Egypt), Countering the Use of the Internet for Terrorist Purposes (India and UAE), Building Law Enforcement Capacity (Brazil and Ethiopia), and Countering the Financing of Terrorism (South Africa).

I would like to distinguish the CTWG subgroup on countering foreign terrorist fighters, co-chaired by Russia and Iran.

This is undoubtedly an urgent threat: it is estimated that since 2011, approximately 50,000 jihadists from over 100 countries have passed through hostilities in Syria and Iraq. Many of these individuals are now returning to their home countries or relocating elsewhere. It is imperative that they do not escape accountability.

It is obvious that international terrorist fighters are catalysts of terrorist violence. As trained combatants with skills in explosives, sabotage, and guerrilla tactics, they pose a serious threat to socio-political stability.

Under the initiative of Russia's chairmanship, the subgroup arranged for BRICS members a series of virtual briefings on FTFs-related issues by relevant United Nations bodies. The first such event, held on February 8, 2022, was an online briefing with the UN Office of Counter-Terrorism. A second briefing took place on June 1, 2023, with experts from the UN Security Council Committee Monitoring Group 1267/1989/2253. This constructive practice will be continued.

The subgroup also conducts analysis of national legislation on FTFs across BRICS countries. Russia has compiled a collection of legal acts currently in force in member states on this matter.

I would like to note the special contribution of the FFMS to the CTWG operation and especially its sub-group on Countering the Financing of Terrorism (CFT). This subgroup engages in substantive discussions on mechanisms for identifying and disrupting financial channels and sources used by terrorists, and addresses issues such as money laundering and the misuse of cryptocurrencies for illegal purposes.

FFMS officers traditionally take an active part in CTWG meetings, engage in discussions, and implement relevant projects to identify terrorist financing sources. In July 2024, the CFT subgroup met to announce a typological study on the activities of ISIS*, Al-Qaeda*, and affiliated groups in BRICS countries. Our partners in the association showed great interest in contributing to this initiative.

The International Training and Methodology Center for Financial Monitoring (ITMCFM) plays a significant role in building human resources capacity for counter-terrorism cooperation among BRICS states. The Center regularly provides training for representatives of financial intelligence units from BRICS states. Last year, experts from Egypt, I.R.Iran, UAE, and Ethiopia underwent training to enhance their qualifications. Also, the ITMCFM and the International Network AML/CFT Institute (INI) organized a series of education and career fairs in AML/CFT in Addis Ababa, Dubai, Cairo, and Rio de Janeiro. Such events are focused on promoting higher education in the field of financial security and help young people learn more about educational opportunities available in Russia.

This year Brazil will host the 10th anniversary meeting of the CTWG. The focus will be on preventing radicalization that leads to terrorism and extremism. We fully support this initiative, especially as Russia has relevant experience to share, including through the new Strategy for Countering Extremism in the Russian Federation adopted in December 2024. We also anticipate valuable contributions from BRICS to a project initiated by Russia in cooperation with the UN Office of Counter-Terrorism. This project aims to examine the extremism phenomenon and explore national and regional approaches to countering this threat.

Our partners from Brazil have also scheduled several other important events that will contribute to the positive trend in BRICS counter-terrorism cooperation. Russia stands ready to fully support this initiative.

«I would like to note the special contribution of the FFMS to the CTWG operation and especially its sub-group on Countering the Financing of Terrorism (CFT). This subgroup engages in substantive discussions on mechanisms for identifying and disrupting financial channels and sources used by terrorists, and addresses issues such as money laundering and the misuse of cryptocurrencies for illegal purposes.

* Designated as terrorist organizations, activities are banned in the Russian Federation.

CSTO'S REGIONAL OPERATION "NELEGAL" (ILLEGAL MIGRANT): ROLE OF FINANCIAL INTELLIGENCE UNITS

Nowadays, illegal migration represents a global challenge. In light of ongoing military and political conflicts and disparities in social and economic development across countries, migratory processes are increasing - often in an uncontrolled manner

SERGEY GONCHAR
Deputy Head of the Challenges and Threats Counteraction Department of the CSTO Secretariat, Associate Professor, PhD in history

Illegal migration within CSTO's area of responsibility is of particular concern among the numerous risks and challenges tackled by this body.

Alongside combatting international terrorism, extremism, drug and arms trafficking, and transnational organized crime, the issue of countering illegal migration is outlined in Article 8 of the CSTO Charter and regulated through a number of legal acts adopted by the Collective Security Council, Committee of Secretaries of Security Councils, and Coordination Council of Heads of Competent Authorities of CSTO Member States on Combating Illegal Migration.

Nowadays, illegal migration represents a global challenge. In light of ongoing military and political conflicts and disparities in social and economic development across countries, migratory processes are increasing - often in an uncontrolled manner. The consequences of unchecked migration are particularly evident in Western European countries, where new ethnic communities and groups have formed. Some of their members do not adhere to established laws and norms of behavior, fostering environments conducive to criminal activity.

In this context, each state must create mechanisms to manage incoming migration to maintain socio-economic and political stability, ensure public order, and safeguard national security.

This is especially relevant to CSTO member states, whose geographical

positions make them transit zones for migrants traveling from the Middle East, Central Asia, Africa to Western Europe, Canada, the USA or settling illegally within CSTO territories for accomplishing their interests, mostly economic.

These processes are often facilitated by organized transnational criminal groups engaged in shadow commercial activity that is closely linked to human trafficking, terrorism, economic crime, and the smuggling of drugs and arms.

One of the CSTO's effective tools for countering illegal migration is the regional Operation Illegal Migrant. It is conducted by the Coordination Council of Heads of Competent Authorities of the CSTO Member States on Combating Illegal Migration. This operation became a permanent fixture in 2017.

Over the past 17 years, Operation Illegal Migrant has been distinguished by its comprehensive approach and coordinated efforts of law enforcement, migration, border control, and special services. These efforts aim to enforce migration laws, expose criminal offenses, and identify those organizing illegal migration and human trafficking.

Through joint activities under Operation Illegal Migrant, CSTO member state agencies regularly detect and dismantle new migration channels from third countries, while preventing the criminal activities of individuals and organized groups, including transnational networks.

A comprehensive approach, as well as a high degree of cooperation between the competent authorities of the CSTO member states, yield significant results in combating illegal migration.

> 2.1 million

violations of migration legislation have been suppressed during 17 years of coordinated actions of competent authorities of CSTO member states

More than 7.7 thousand wanted persons have been detained, and about 270 thousand foreign nationals have been deported or administratively expelled. More than 35 thousand criminal cases have been initiated for the organization of illegal migration.

More than 144 thousand criminal cases have been initiated in connection with other crimes uncovered during regional CSTO operations, including:

- Over 32.7 thousand cases linked with drug trafficking;
- Over 5.3 thousand cases linked with arms trafficking;
- Over 2.8 thousand violations of state borders;
- 154 extremist and terrorist-related offenses.

This year, Operation Illegal Migrant is being conducted in 2 stages, involving all relevant law enforcement structures and financial intelligence units of CSTO member states.

Financial intelligence units of CSTO member states play an important role in the preparation and conduct of the operation. These agencies conduct macroeconomic analyses of suspicious financial transactions involving foreign nationals, examine financial investigation files to identify non-resident individuals, and uncover and block accounts and assets potentially linked to criminal networks engaged in illegal migration.

Their coordinated efforts have produced tangible results. Since 2018, as part of the CSTO's Operation Illegal Migrant, financial intelligence units have conducted 39 financial investigations, revealing more than 7,600 suspicious transactions totaling over USD 103 million.

An important milestone in the fight against money laundering, terrorist financing, and transborder organized crime was the signing of the Protocol of Cooperation between the Council of Heads of Financial Intelligence Units of the CIS Member States (CH FIUs) and the Secretariat of the Collective Security Treaty Organization signed on May 29, 2019.

« The operations carried out over the past 17 years have been marked by their comprehensive nature, coordinated efforts involving police, migration, border control, and special services. These efforts focus on monitoring compliance with migration legislation, detecting related crimes, and exposing the organizers of illegal migration and human trafficking.

The Protocol establishes the following forms of cooperation:

- Exchange of information on mutually relevant issues;
- Sharing of experience through joint conferences, seminars, and other events;
- Formation of joint working groups, when necessary, to develop proposals on high-priority matters;
- Participation in events and meetings organized by CH FIUs or the CSTO Secretariat related to each party's area of interest;
- Joint publications.

It is especially important to enhance measures aimed at detecting, suppressing, and documenting the laundering of proceeds from illegal migration, while leveraging the capabilities of CH FIUs and the EAG in this work.

To raise the effectiveness of these efforts, representatives of the International Organization for Migration Bureau in Moscow participated in consultations on developing new approaches to combat money laundering related to illicit migration.

In conclusion, I can state with confidence that the work of the financial intelligence units of CSTO member states not only supports the fight against illegal migration and related money laundering but also reinforces financial security throughout the CSTO area of responsibility.

The laundering of criminal proceeds from illegal migration continues to evolve, adapting to the countermeasures employed by CSTO member states.

MADAGASCAR FACING TERRORISM: BUILDING AN EFFECTIVE DYNAMIC

MAMITIANA RAJAONARISON
Head of financial intelligence unit of the Republic of Madagascar

> Terrorism is one of the major universal concerns of the world today. Indeed, rich or developing countries, North or South, East or West are all confronted in one way or another with this phenomenon which is deeply harmful to humanity.

Any nation may serve as a target, a transit point, a refuge, or a site for the planning of terrorist activities. In response, the United Nations (UN) has enacted a number of conventions and resolutions with the aim of encouraging countries to prevent, combat and repress this phenomenon.

After several years, particularly following the events of September 11, 2001, the Financial Action Task Force (FATF) shifted its focus to this significant concern. The Group thus incorporated recommendations targeting the financing of terrorism to its standards. This approach aims to impede the operational effectiveness of terrorist groups, aid in their identification after attacks, and, most importantly, diminish their overall power.

The fight against terrorism is significantly complicated by the fact that its funding can originate from both illicit and legitimate sources.

As a member of the UN and the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), Madagascar has a legal and institutional arsenal to contribute to this fight. There are two main laws that govern the fight:

- Law No 2014-005 on the fight against terrorism and transnational organized crime
- Law No 2018-043 amended and supplemented by Law No 2023-026 on the fight against money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

The defense and security forces are equipped with counter-terrorism units. Additionally, Madagascar hosts an INTERPOL National Central Bureau, which serves as a significant entity and a robust connection to international intelligence networks.

In order to improve the effectiveness of the fight against transnational organized crime including terrorism, terrorist financing and money laundering, the various entities involved engage in daily collaboration. For instance, INTERPOL, SAMIFIN (Financial Intelligence Unit)

and the Directorate of Migration Control have established bilateral Memoranda of Understanding for the exchange of information. These arrangements grant access to specific INTERPOL databases such as: the Stolen and Lost Travel Documents (SLTD), the Interpol Criminal Information System (ICIS), the Travel Documents Associated With Notices (TDAWN), and the Forensic Investigations and Documentation (FIND) among others. Additionally, both the gendarmerie and the national police maintain dedicated investigative units focused on cybercrime, which is addressed under law No 2014-006 amended and supplemented by Law No 2016-031. The use of new technologies for the purposes of terrorism or terrorist financing therefore falls within the scope of national legislation.

Some of the results achieved in 2024 attest to Madagascar's effectiveness in the fight against terrorism and its financing. This concerns the use of INTERPOL databases:

- No individual listed by INTERPOL has transited through Madagascar (entry and exit from the territory);
- An individual from a neighboring country known to be a terrorist hotspot was turned back at his airport of departure because his travel document (passport) had been reported lost;
- The SLTD database was fed by 1,704 Malagasy passports that have been reported lost, stolen or revoked. This reflects increased vigilance by the Malagasy authorities regarding the potential misuse of these documents for illicit activities;
- The operationalization of FIND, which provides access to ICIS, SLTD and TDAWN, has resulted in over 1,800,000 active consultations with INTERPOL databases for preventive and control measures. Madagascar has thus attained the 11th position in Africa regarding the consultation of INTERPOL databases.
- This same FIND system generated a total of 136 reports concerning the border movements of individuals recorded with INTERPOL's ICIS, SLTD, and TDAWN databases.

Furthermore, as part of the strengthening of human capital engaged in Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT), a research and training center has just been set up within SAMIFIN. Bridging knowledge and practice, this center will also share good practices in the fight against financial crimes. It will implement a comprehensive training program focused on systematic financial investigation techniques, which will run concurrently with investigations and prosecutions related to transnational organized crime, including terrorism and various forms of trafficking.

In conclusion, fully committed to never appearing as a refuge or a rear base for criminal and terrorist activities, Madagascar remains a land of peace and security fostering harmonious coexistence both within and with the world community, thereby positioning itself among the foremost contributors to the welfare of humanity.

INTERAGENCY ANTITERRORIST COOPERATION IN THE EURASIAN GROUP (EAG):

MUTUAL BENEFITS OF I.R. IRAN AND THE EAG FROM COLLABORATIVE EFFORTS

The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), established in 2004, is a shining example of regional collaboration against financial crimes of terrorism financing.

MORTEZA PARVANEH SHAMAMI
International law expert

Modeled on the Financial Action Task Force (FATF), it unites nine countries — Belarus, China, India, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan, and Uzbekistan — to safeguard the standard financial systems and guarantee security beyond borders. For I.R. Iran, an observer member of this elite group, collaboration with the EAG is a proud step towards deeper collaboration with our Eurasian allies. This essay explores the interagency collaboration mechanisms within the EAG, I.R. Iran's growing role, and celebrates the mutual benefits this collaboration offers to our shared combat against terrorism financing.

THE EAG'S FRAMEWORK: A RESPECTFUL SPACE FOR COOPERATION

We in I.R. Iran value the EAG framework since it permits collaboration while every nation retains sovereignty. The EAG Plenary, a meeting of the representatives of financial intelligence units (FIUs), law enforcers, and regulatory agencies, provides a platform for decision-making and discussion. Guided by working groups — such as the Working Group on Typologies (WGTYP), which looks at trends in terrorism financing — the EAG provides a platform where actionable intelligence is exchanged, and policy is aligned — and having a conscientious Secretariat in Moscow, the EAG keeps everything focused and on target. This works with us, as it reconciles shared objectives with the autonomy of each member.

To I.R. Iran, for whom guarding sensitive information is a matter of national pride and security concern, the EAG's emphasis on mutual evaluation and technical assistance appears measured and respectful. The evaluations offer suggestions for improvement without overstepping boundaries, and training sessions

enhance our capabilities discreetly. In Central Asia, where issues such as illicit trade and border intricacies continue to exist, the EAG's efforts — such as the Central Asian Regional Information and Coordination Centre (CARICC) — demonstrate how cooperation can make us all more resilient, provided it honors each nation's unique circumstances.

I.R. IRAN'S HONORABLE ROLE IN THE EAG

As an observer state among 17 nations and 24 international organizations, I.R. Iran is increasingly privileged to interact with the EAG. This allows us to participate in plenary sessions, learn from exchanged experiences, and collaborate on a noble cause with reliable partners such as The Russia and China, which established the group. Our involvement is evidence of our historical connection with Eurasia and our interest in regional stability, further solidified by our 2023 Shanghai Cooperation Organization (SCO) membership.

Economically, I.R. Iran's ties with the EAG thrive under plans such as the free trade agreement (FTA) with the Eurasian Economic Union (EAEU), which we signed in December 2023.[1] The deal that has brought us nearer to EAG members Kazakhstan, Kyrgyzstan, and Russia encompasses almost 90% of goods and paves the way for prosperity through lawful trade. Such ties are achievable under cooperation possibilities that are considerate of our financial sovereignty and the objectives of the EAG. Politically, our presence highlights I.R. Iran's commitment to a safe Eurasia, contributing our vision and expertise to build a future where terrorism is not a concern.

MUTUAL BENEFITS: A PARTNERSHIP ROOTED IN RESPECT

Collaboration with the EAG is a matter of pride and strength from the I.R. Iranian viewpoint, and its benefits are reciprocal. To the EAG, I.R. Iran offers extensive regional experience developed by virtue of our strategic position and deep understanding of economic flows across borders. We would be ready to exchange experiences in ways that respect our domestic laws and principles. This alliance enhances the EAG's ability to deter threats, provided that it is an equal partnership sensitive to our national interests.

To I.R. Iran, the EAG offers valuable instruments to make our antiterrorist efforts more effective. Under observer status, we benefit from training and best practices to improve our FIU's effectiveness — efficiently and unobtrusively, without compromising our autonomy. Financial monitoring initiatives, tailored to our needs, allow us to protect our economy from exploitation according to international criteria as we deem appropriate. This exchange of expertise is a testament to the respect the EAG has for our sovereignty, fostering trust in our shared mission.

Strategically, I.R. Iran's participation elevates the EAG's stature as a unified Eurasian voice. Supported by The Russian Federation, together, we craft a multipolar space that honors plural perspectives, addressing external pressures with elegance. For I.R. Iran, this alliance lends voice to our influence in regional security, allowing us to stand shoulder-to-shoulder with allies in a shared fight against terrorism. It is an alliance that reflects our ideals — cooperation without coercion, unity without intrusion.

An excellent instance of such interagency collaboration was the first Joint EAG and CIS CCPG Forum of Prosecutors on AML/CFT, organized in Minsk, Republic of Belarus, on 13-14 November. At the Forum, where I had the privilege of representing the FIU of I.R. Iran, delegations spoke about the role of prosecution authorities in strengthening national AML/CFT systems, their role in combating terrorist financing and money laundering, international cooperation in the recovery of criminal assets, tackling new challenges in mutual legal assistance, and involvement in national interagency AML/CFT frameworks. The delegates to the Forum exchanged national practice in the development of interagency interaction between prosecutor's offices and financial intelligence units, asset recovery operations, initiatives to strengthen legal regulation of anti-criminal cooperation, arrangements for electronic communication in mutual legal assistance and other cooperation, counteraction to regional ML/TF risks, and utilization of virtual assets for criminal activity.

BUILDING A STRONGER FUTURE TOGETHER

I.R. Iran and the EAG need to sustain trust to reinforce this virtuous connection. For the EAG, accepting I.R. Iran's application for deeper engagement — full membership — would acknowledge our contributions while respecting our pace. Mechanisms of confidential dialogue, instead of non-relevant data requests, would ease coordination, allowing our expertise to enhance the group's efforts. Joint training on new challenges, such as digital currencies, would further harmonize our capabilities in a spirit

[1] https://eec.eaeunion.org/en/comission/department/dotp/torgovye-soglasheniya/iran.php.

of two-way learning. On its side, I.R. Iran can receive EAG assets to reinforce our defenses, accepting tools and frameworks suitable to our circumstances.

By actively participating in forums, we can take the lead on protecting trade routes and exchanging knowledge without diluting our national principles. With partners such as the United Nations Office on Drugs and Crime (UNODC), we can shape support to fit us so that this partnership continues to be a source of strength. UNODC, as an international agency, can play a significant role in enhancing regional cooperation against terrorism. By providing technical assistance, such as training for security and judicial personnel, the UNODC strengthens local capacities to address terrorist threats effectively. We also acknowledge the initiative of the Russian Federation ITMCFM that plays such an important role in AML/CFT through the development of expertise, regional collaboration, and technological innovation.

« Based on respect and consideration for our values, this collaboration strengthens Eurasian resilience against terrorism financing. By building trust and maintaining relations, the EAG and I.R. Iran can build a future with flourishing cooperation, particularly in antiterrorism, and protect our lands with dignity and unity.

CONCLUSION

Interagency antiterrorist collaboration in the EAG is a noble cause, bringing countries together in a common pursuit of safety while upholding the dignity of each member. As of February 20, 2025, I.R. Iran's increasing role in this group is a source of pride, with the benefits being reciprocal: regional expertise to the EAG and technical empowerment for I.R. Iran. Based on respect and consideration for our values, this collaboration strengthens Eurasian resilience against terrorism financing. By building trust and maintaining relations, the EAG and I.R. Iran can build a future with flourishing cooperation, particularly in antiterrorism, and protect our lands with dignity and unity.

The views and opinions expressed in this content are solely those of the author and do not necessarily reflect the views or policies of the Islamic Republic of I.R. Iran or the INFIC.

EAG NEWSLETTER INITIATIVE ON TERRORIST GROUPS' ACTIVITIES

In May 2024, EAG member states, recognizing the dynamic changes in how terrorist organizations finance their activities, agreed to launch a project for developing an information bulletin on the activities of terrorist groups in the Eurasian region.

IVAN ANISIMOV
Representative of the Federal Financial Monitoring Service

Al-Qaeda* and Islamic State*, Khorasan Province* and Al-Nusra Front*, Tehreek-e-Taliban-e-Pakistan* and Turkistan Islamic Party* are designated terrorist organizations. What do they have in common? How did they emerge? Why do they commit terrorist acts? What are their goals and motivations? Where do they recruit new members?

These are serious questions that must be addressed to fully comprehend the logic of what constitutes the primary global threat - international terrorism. A common mistake in analyzing terrorist organizations - whether global or regional - is assuming that their tactics and strategies follow a uniform pattern.

While terrorist groups operating in specific geographic areas may exhibit similar features, their objectives and the methods they use to achieve them often differ significantly.

A clear example of this is the contrast between ISIS* and Al-Qaeda* - arguably the two most notorious terrorist organizations in the world. Their differences are rooted in their fundamental ideological foundations.

Osama bin Laden, leader of Al-Qaeda*, believed his actions were only a prelude to the eventual establishment of a Caliphate. His principal objective was to "ignite the spark" that would ultimately lead society to that goal.

Under his leadership, Al-Qaeda* adopted a decentralized network model. In contrast, the Islamic State* adheres to the belief that the Caliphate must be established immediately. It views the acquisition and governance of physical territory as central to its mission. The organization implements a centralized administrative structure, with clearly defined military and civilian branches and territorial divisions known as vilayats (provinces).

Understanding these distinctions, along with key ideological narratives - such as the eschatological importance of Dabiq, referenced by ISIS* as the prophesied site of an ultimate battle in Syria - is critical to analyzing the unique characteristics of each group. These distinctions underscore that even major terrorist organizations differ in significant and strategically relevant ways.

Fully recognizing this complexity and the ongoing evolution in how terrorist organizations generate and manage their financial resources, member states of the Eurasian Group on Combating Money Laundering and Financing of Terrorism agreed in May 2024 to launch a dedicated information bulletin. This publication will systematically document the activities of terrorist organizations in the Eurasian region.

Years of collaborative research into money laundering and terrorist financing (ML/FT) typologies have enabled member states to raise awareness of terrorist threats, establish cooperative response mechanisms, and later effectively implement programs to adjust national anti-money laundering legislation.

For instance, initiatives have targeted methods used by individuals associated with terrorist activities, such as purchasing airline tickets, sources of funding for illegal activities, including proceeds from organized crime, and the integration of specific tools into national laws to counter terrorism financing, such

as asset-freezing procedures for persons linked to terrorism.

However, to date, the EAG has not undertaken a project to identify connections between terrorist organizations common to all member states and those specific to individual states. The EAG's current initiative focuses on uncovering links between terrorist groups and their associated financing techniques and methods. Numerous typological studies have accumulated substantial factual elements; however, no comprehensive analysis has yet been conducted in the Eurasian region to compare all operational aspects of specific terrorist groups active in the area.

This gap is underscored by emerging trends where previously rival terrorist groups are not only reducing conflicts among themselves but, in some instances, collaborating to pursue joint objectives. This trend has also been noted by the international community. There is increasing movement of fighters from other countries and even continents to participate in combat operations of international terrorist organizations (ITOs), while communication and coordination methods among these groups continue to evolve.

Summarizing all of the above, EAG member states approved the bulletin project endeavor. In November 2024, the EAG analyzed activities of a number of terrorist organizations that pose the greatest threat to the member states.

By examining migration patterns and the locations of terrorist bases, the project seeks to map the geographical expansion of ITOs, which is critical to developing a robust regional security framework. For instance, had the international coalition recognized the intentions of ITOs like ISIS* and Al-Qaeda* during the power vacuum in the Middle East and North Africa following the Arab Spring, many adverse consequences for the region could have been mitigated. Notably, terrorist-affiliated groups crossed the Syrian-Iraqi border to perform subversive actions well before major invasions, securing funding through financial networks that directly exploited instruments of the Iraqi banking system.

Geographical analysis remains a key tool in identifying the primary funding sources for international terrorist organizations. Monitoring changing trends and detecting hotspots early can disrupt emerging asset supply chains. Ongoing research has already identified specific electronic services, such as mobile applications, used by members of ITOs for criminal purposes. The set of these applications vary by organization and is closely tied to the nature and characteristics of each ITO's activities.

The project is actively progressing, with all parties recognizing it as the initial phase of a broader effort, as the research reveals new connections between terrorist groups across countries and continents.

* Designated as terrorist, activities banned in the Russian Federation.

KAZAKHSTAN'S EXPERIENCE IN INTERNATIONAL COOPERATION AGAINST TERRORIST FINANCING

Countering the financing of terrorism remains a critical challenge to global security. Addressing this threat requires robust cooperation with neighboring states and the international community.

SALTANAT BAISBAY

Chief Consultant of the Department of Financial Monitoring of Terrorism Financing, Drug Trafficking, and Proliferation of Weapons of Mass Destruction of the Financial Monitoring Agency of the Republic of Kazakhstan.

Kazakhstan's financial intelligence unit (FIU) plays an active role in international initiatives to counter terrorist financing. It shares data, improves national legislation, and implements new financial monitoring methodologies.

In addition, Kazakhstan's FIU cooperates with the FATF, EAG, and CH FIUs in developing global mechanisms to combat terrorist financing.

International cooperation with foreign partners is key in the early detection and prevention of terrorist financing. This includes activities such as information exchange, joint analysis endeavors, etc.

For example, joint efforts of Kazakhstan's FIU and the Czech Republic partners led to the disruption of a financing channel for the banned extremist religious organization Takfir wal-Hijra* and the conviction of 12 of its supporters.

A parallel financial investigation allowed to identify an ideological supporter of Takfir wal-Hijra*, as well as foreign bank cardholders and financial backers of this International Terrorist Organization (ITO).

As a result of this cooperation with the Czech FIU, criminal proceedings were initiated.

It is important to promote information exchange and enhance international cooperation to ensure global security, advance mutual interests, and help maintain international financial security.

We believe that only through close collaboration among all stakeholders within national anti-money laundering frameworks can we effectively combat money laundering and prevent terrorist financing.

Global security is only possible with the close cooperation of countries.

* Designated as extremist, activities banned in the Russian Federation.

INTER-AGENCY PARTNERSHIP IS KEY TO LONG-TERM COUNTER-TERRORISM SUSTAINABILITY: NATIONAL EXPERIENCES

ESTABLISHMENT OF NATIONWIDE COUNTER-TERRORISM SYSTEM IN RUSSIAN FEDERATION

EVGENY ILYIN

Advisor to the Chairman of the National Anti-Terrorism Committee, Deputy Head of the Expert Coordination Group on Countering the Financing of Terrorism and Extremism at NATC, PhD in Law

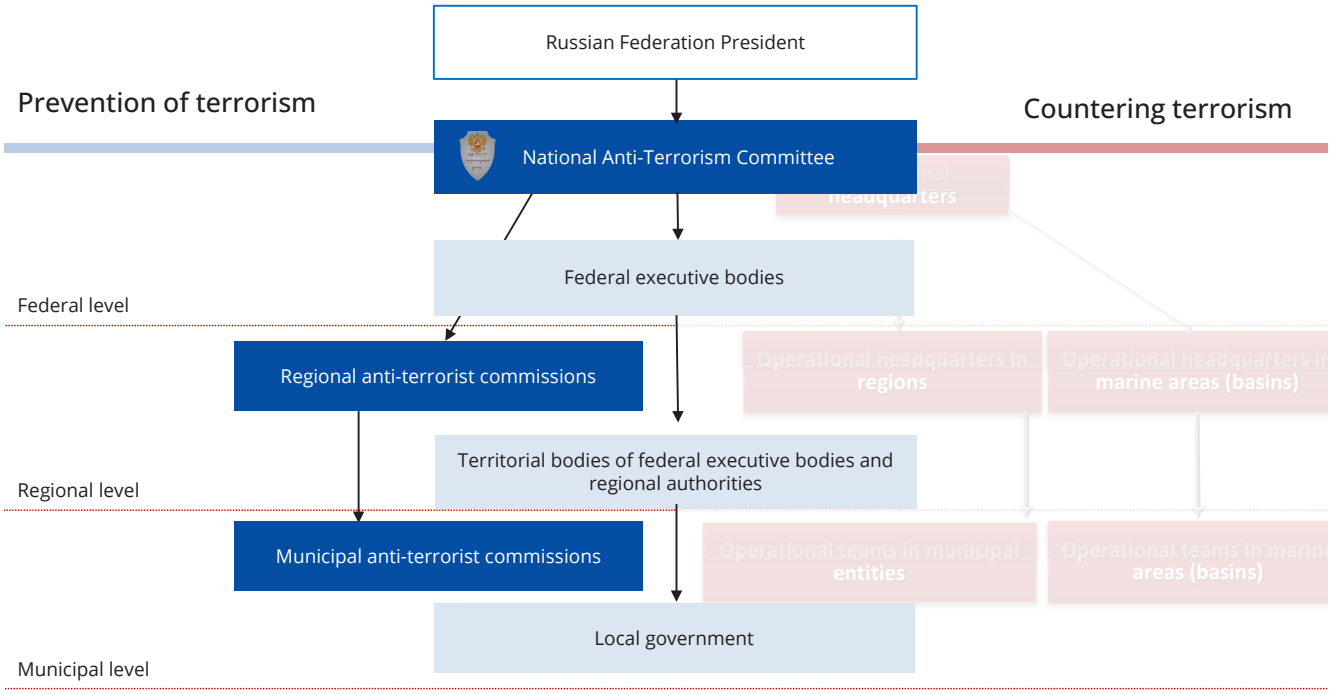
The article is devoted to the Russian experience in establishing a nationwide counter-terrorism system[1]. Particular emphasis is placed on the development of a comprehensive system to counter terrorism and terrorist financing, assessing its effectiveness, and outlining the principles of the National Anti-Terrorism Committee (NATC) as the core entity of the NCTS, which operates based on a permanent inter-agency partnership.

At the turn of the 21st century, terrorism as a social phenomenon has acquired a global character. The Russian Federation was one of the first countries to face its aggressive manifestations, incited by international terrorist organizations, and suffered significant human losses. In response to this threat to its territorial integrity and very statehood, Russia was compelled to rapidly reform its counter-terrorism strategy. This involved mobilizing all state institutions and civil society to develop a fundamentally new nationwide counter-terrorism system.

At the turn of the 21st century, Russia faced the aggression of international terrorism

[1] NCTS.

Nationwide Counter-Terrorism System



Core principles of the Russian NCTS established in 2006 by the Federal Law On Countering Terrorism[2], Decree of the Russian President On Counter-Terrorism Measures[3], and Concept of Countering Terrorism in the Russian Federation: approved by President in 2009[4].

With this, let's review the principles of the NCTS structure and counter-terrorism techniques, underlying the development and operation of this system: a shift from combating terrorism to comprehensive counter-terrorist efforts that includes, in addition to combating, preventive measures, and measures to mitigate and eliminate the consequences of terrorist activities. Effective operation of this system requires effective inter-agency partnership.

Core principles that form the basis of the modern NCTS in the Russian Federation include:

1. A comprehensive approach to counter-terrorism in three key areas:

- Combating terrorism;
- Preventing terrorism by identifying and eliminating root causes and conditions conducive to terrorist attacks;
- Mitigating and eliminating the consequences of terrorist acts.

In recent years, Russia has placed increasing emphasis on preventing terrorism and countering terrorist ideology.

Why these three directions? First, relying solely on force to combat terrorism is insufficient. To truly defeat terrorism, its ideology must be challenged to prevent recruitment - especially among youth and other vulnerable groups.

Second, government institutions alone cannot effectively combat terrorism. Public and religious organizations, academic and creative community, and respected public figures must be involved in the fight against terrorists. Therefore, the unity between the state and society is essential in addressing this global problem.

2. Clear division of competencies in countering terrorism among different government agencies and their leadership.

[2] On Countering Terrorism: Federal Law dd. June 03, 2006 No. 35-FZ // Corpus of Legislation RF 2006 No. 11 Art. 1146.
[3] On Counter-Terrorism Measures: Decree of the Russian President dd. February 15, 2006 No. 116 // Corpus of Legislation RF. 2006. No. 8 Art. 897.
[4] Concept of Countering Terrorism in the Russian Federation: approved by the Decree of the Russian President dd. October 0, 2009 // Rossiyskaya Gazeta 2009 No. 198.

This ensures personal accountability.

Prior to the establishment of the NCTS, it was common for senior officials to delegate counter-terrorism responsibilities to deputies lacking the necessary authority or capacity to act. This often led to delays in implementation of the decisions made at the meetings due to the lengthy follow-up coordination - unacceptable amid escalating terrorist threats - and ultimately weakened the overall counter-terrorism system.

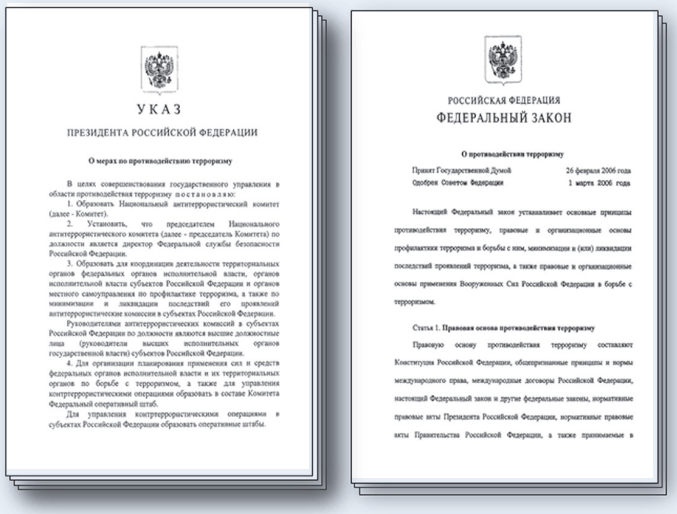
3. Decisions of the National Anti-Terrorism Committee[5] and the Federal Operational Headquarters (FOH)[6] are binding for all government institutions, public organizations, and citizens.

- **NATC decisions are mandatory for all state bodies, legal entities, and individuals**
- **Failure to implement NATC decisions is subject to administrative liability**
- **Since 2016, decisions of anti-terrorist commissions have also held binding legal status**

This is one of the most important and fundamental features of the new system. Naturally, public awareness, understanding, and acceptance of the NATC are gradual processes: no single institution can claim to solve all problems in this area at once, especially across various levels of state and municipal administration. Initially, the binding nature of decisions was extended to the NATC, the FOH, and operational headquarters at the regional and maritime (basin) levels[7]. Subsequently, this authority was extended to regional anti-terrorist commissions (ATCs), and finally, to municipal anti-terrorist commissions[8]. Only after that, decisions of municipal anti-terrorist commissions acquired binding status.

This progressive expansion allowed for increased oversight of the implementation of decisions issued by operational headquarters and anti-terrorist commissions, along with the introduction of administrative penalties for failure to comply.

Nationwide Counter-Terrorism System


УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ
О мерах по противодействию терроризму

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН
О противодействии терроризму

October 5, 2009

Concept of Countering Terrorism in the Russian Federation, approved by the President of Russia

Key Directions of Countering Terrorism in the Russian Federation


Combating terrorism


Preventing terrorism and its ideology


Mitigating and eliminating the consequences of terrorist attacks

[5] NATC.
[6] FOH.
[7] OH, headquarters.
[8] ATC.

4. Empowering the heads of all coordination bodies (NATC, FOH, ATCs, and operational headquarters) to independently make and implement decisions within their authority. These officials are both entitled and obligated to make independent decisions and immediately proceed with their execution, without requiring additional approvals.

This tool has proven to be effective. Terrorists act covertly and unpredictably, leaving no time and opportunity to prepare in advance for suppressing imminent terrorist threat or specific criminal action. Russian legislation therefore authorizes the head of the local security authority - who often also serves as the head of the regional operational headquarters - to independently initiate anti-terrorist operations[9], impose the legal counter-terrorist regime (with notification to the Center), and immediately begin implementation.

5. The NATC and the FOH are composed exclusively of senior executives (heads of relevant ministries, departments, and other government agencies authorized to make final decisions within their jurisdictions).

This structure applies to the entire NCTS at all levels, including regional and municipal. It enables decisions made at NATC, FOH, ATC, and operational headquarters meetings to be finalized promptly, without lengthy bureaucratic procedures. This model has been effectively applied - for example, when the Head of the Chechen Republic appealed directly to the President of the Russian Federation, leading to the swift termination of the counter-terrorist operation regime following the restoration of constitutional order in the region.

6. Introduction of the principle of unity of command and the assignment of personal responsibility to designated leaders. In the area of terrorism prevention, responsibility is assigned to regional heads; in combating terrorism, it lies with the heads of local branches of the Federal Security Service of Russia.

The principle of unity of command and personal responsibility, previously discussed, has been reinforced over the 19-year history of the NCTS, validating its effectiveness in counter-terrorism efforts.

7. Early development of anti-terrorism procedures and plans and their consistent testing during exercises. Each region conducts at least four exercises per year. Additionally, international anti-terrorism drills are regularly held under the supervision of representatives from foreign states and international organizations.

8. Defining the fundamental areas of NCTS work to facilitate enhanced coordination among relevant government bodies. For this purpose, the Expert Coordination Council and eight Expert Coordination Groups (ECGs) were established under the NATC; one of them is responsible for implementing state policy on countering the financing of terrorism.

This group, like the NATC itself, includes representatives from government agencies and civil society. It operates under NATC's regulatory framework and follows both the Interagency Comprehensive Plan and the ECG Work Plan.

Since 2010, the NATC and the FOH have jointly approved interagency comprehensive action plans to counter the financing of terrorism and extremism for three-year periods. The most recent plan, the Interagency Comprehensive Action Plan for 2025–2027, was reviewed and adopted in December 2024 at a joint NATC and FOH meeting. These plans are binding for all participating agencies whose leaders are members of NATC. Their implementation enables a coordinated and effective national response to terrorist financing.

Main CFT Objectives of the ECG:

- Consolidating the expert community in the fight against terrorism;
- Reviewing operational challenges in the national system for countering terrorist financing;
- Developing proposals to strengthen legislation and improve the national counter-terrorist financing framework.

The ECG is chaired by the Director of the Federal Financial Monitoring Service, with the Advisor to the Chairman of the NATC serving as Deputy Chair. The Group's first meeting was held on December 22, 2009.

Since its establishment, the ECG under the NATC has developed a wide range of initiatives. For instance, on September 26, 2018, the Group's meeting discussed leveraging the potential of the Interagency Commission on Countering the Financing of Terrorism for the purpose of preventing terrorists from exploiting real estate assets. These efforts led to the adoption of Federal Law On Amendments to the Federal

[9] CTO.

Nationwide Counter-Terrorism System

- National Anti-Terrorism Committee
- Federal Operational Headquarters

Alexander Bortnikov, Chairman of the NATC and Head of the FOH, Director of the Federal Security Service of the Russian Federation

23 officers
representing various government agencies are members of the NATC

Law On State Registration of Real Estate and Certain Legal Acts of the Russian Federation No. 120-FZ dated April 30, 2021.

Under this law, the Unified State Register of Real Estate must include information on the freezing (arrest) of assets belonging to persons listed in the official List of Organizations and Individuals Involved in Extremist or Terrorist Activities[10], as well as individuals whose assets have been frozen by decision of the Interagency Commission on Countering the Financing of Terrorism. This data serves as a basis for suspending the registration of affected real estate.

The Expert Coordination Group reviewed the effectiveness of cooperation with financial institutions in countering the financing of terrorism. This included analyzing how organizations that conduct financial transactions respond to asset freezing measures targeting listed individuals and those blocked by the Commission's decisions. At its meeting in the first quarter of 2019, the Group developed Methodological Recommendations implementing asset freezing (arrest) procedures by organizations and individual entrepreneurs involved in financial transactions. These Recommendations, along with Memorandum No. 60 dated March 1, 2019, were published on the official website of the Federal Financial Monitoring Service.

In line with a protocol directive issued on June 7, 2019, aimed at enhancing interagency coordination and effectiveness in combatting terrorism and extremism financing, the Federal Financial Monitoring Service distributed unified methodological guidelines to all relevant authorities. These guidelines outlined practical mechanisms to suppress terrorist financing.

The 46th meeting of the Group considered, among other things, the most common techniques used by terrorists in the Russian Federation to raise, transfer, or use funds for criminal purposes. The findings were incorporated in the National Terrorist Financing Risk Assessment (NTRA). As a result, it revealed vulnerabilities of the Russian CFT system and helped classify terrorist financing risks, which allows to prioritize the areas requiring special attention.

At its 48th meeting, the Group agreed to participate in the FATF typologies study on Crowdfunding for the Financing of Terrorism with Russia contributing its regulatory experience in combating the misuse of crowdfunding mechanisms for criminal purposes.

In addition, analysis of terrorist organizations' financial operations remains essential to dismantling their material support systems. The Group formulated a set of targeted questions for collaboration with international partners under the EAG platform. Based on a decision at its 51st meeting, Russia is currently compiling and presenting consolidated information on five terrorist organizations active in the Eurasian region as part of a new bulletin project.

These efforts highlight the essential characteristics of the NCTS, which has been active in the Russian Federation for the past 19 years.

Russia's approach - centered on systematic, evidence-based measures - has successfully reduced terrorist threats and activity. This success has been recognized by the public and international bodies, including the United Nations Security Council's Counter-Terrorism Committee (CTC UNSC).[11]

[10] The List.
[11] CTC UNSC.

RANK	COUNTRY	SCORE	RANK CHANGE
1	Afghanistan	8.822	↔
2	Burkina Faso	8.564	↑ 2
3	Somalia	8.463	↔
4	Mali	8.412	↑ 3
5	Syria	8.161	↑ 1
6	Pakistan	8.160	↑ 3
7	Iraq	8.139	↓ 5
8	Nigeria	8.065	↓ 3
9	Myanmar (Burma)	7.977	↑ 1
10	Niger	7.616	↓ 2
11	Cameroon	7.347	↑ 1
12	Mozambique	7.330	↓ 1
13	India	7.175	↔
14	Democratic Republic of the Congo	6.872	↑ 2
15	Colombia	6.697	↓ 1
16	Egypt	6.632	↓ 1
17	Chile	6.619	↑ 1
18	Philippines	6.328	↓ 1
19	Chad	6.168	↔
20	Kenya	6.163	↔
21	Iran	5.688	↑ 5
22	Yemen	5.616	↓ 1
23	Türkiye	5.600	↔
24	Indonesia	5.502	↔
25	Israel	5.489	↑ 5
26	Thailand	5.430	↓ 4
27	Togo	4.915	↑ 49
28	Benin	4.840	↑ 23
29	Sri Lanka	4.839	↓ 4
30	United States of America	4.799	↓ 2
31	Greece	4.793	↓ 2
32	Libya	4.730	↓ 5
33	Palestine	4.611	↓ 1
34	France	4.419	↑ 2
35	Germany	4.242	↓ 4
36	Nepal	4.134	↓ 2
37	Algeria	4.083	↑ 3
38	Tanzania	4.065	↓ 3
39	Burundi	4.051	↓ 6
40	Tunisia	3.989	↓ 1
41	Peru	3.856	↓ 3
42	United Kingdom	3.840	↓ 5
43	Bangladesh	3.827	↓ 2
44	Djibouti	3.800	↑ 52
45	Russia	3.799	↓ 1
46	New Zealand	3.776	↓ 4
47	Côte d'Ivoire	3.747	↓ 4
48	Uganda	3.599	↓ 3
49	Norway	3.514	↑ 31
50	Tajikistan	3.438	↓ 3
51	Venezuela	3.409	↓ 5
52	Lebanon	3.400	↔
53	Italy	3.290	↓ 3
54	Canada	3.275	↓ 6
55	Central African Republic	3.194	↑ 12
56	Ethiopia	3.044	↓ 7
57	Argentina	2.875	↔
58	Slovakia	2.784	↑ 38
59	Belgium	2.763	↑ 11
60	Spain	2.712	↓ 5
61	Austria	2.677	↓ 8
62	Japan	2.398	↑ 12
63	Saudi Arabia	2.387	↓ 9
64	Sweden	2.307	↑ 7
65	Switzerland	2.205	↓ 9
66	Ecuador	2.198	↓ 8
67	Netherlands	2.120	↓ 8
68	Jordan	2.033	↓ 8
69	Australia	1.830	↓ 8
70	Uzbekistan	1.731	↑ 26
71	Paraguay	1.605	↓ 7
72	Mexico	1.578	↓ 10
73	Ukraine	1.535	↓ 10
74	Cyprus	1.392	↓ 8
75	Malaysia	1.357	↓ 7
76	United Arab Emirates	1.241	↑ 20
77	Senegal	1.108	↓ 5
78	Eswatini	1.058	↓ 5
=79	Bahrain	0.826	↓ 14
=79	Rwanda	0.826	↓ 3
=79	South Africa	0.826	↓ 3
=79	Uruguay	0.826	↓ 4

GLOBAL TERRORISM INDEX 2023 |

Following its 2012 visit to Russia, the CTC Executive Directorate recommended that Russia's counter-terrorism practices be promoted internationally. Notably, according to the Global Terrorism Index, Russia improved its ranking from 9th in 2011 to 45th in 2022 - a 36-point improvement in its ability to counter terrorism.[12]

A brief review of national experience in countering terrorism does not cover the entire range of tools used by government agencies and civil society institutions in this area. Moreover, ongoing refinements to this work are required over time, enabling Russia to respond adequately to emerging hotspots of terrorist threats, particularly in the context of the Special Military Operation, and to enhance preventive strategies and methodologies. One constant remains: the consistent, targeted nature of Russia's counter-terrorism work, focused firmly on preventing terrorist acts and extremist manifestations, deterring the involvement of Russian citizens in terrorism, and building societal resilience.

The fundamental instruments of the United Nations, the UN Security Council, and the Counter-Terrorism Committee will continue to serve as the legal platform for international cooperation in countering terrorism.

[12] See Global Terrorism Index: http://reliefweb.int/report/world/global-terrorism-index-2022.

ASSESSING TERRORIST FINANCING RISKS IN KYRGYZ REPUBLIC

Terrorist financing is a complex transnational threat that requires constant monitoring and rapid response. The risk assessments - in particular the national risk assessment - examined the key channels of terrorist financing in the Kyrgyz Republic, their evolution, and modern methods of counteraction.

KANAT ASANGULOV
Chairman of the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic

Countering the financing of terrorism remains a critical challenge to global security. Kyrgyzstan, as part of the global community, faces challenges stemming from illicit financial flows that support terrorist organizations. This illicit activity is a complex transnational threat that requires constant monitoring and rapid response. The risk assessments, in particular the national risk assessment, examined the key channels of terrorist financing in the Kyrgyz Republic, their evolution, and modern methods of counteraction. Based on the data, measures to enhance financial monitoring were proposed and approved by the Commission for countering the financing of terrorism and combating money laundering of criminal proceeds (CFT/CML) under the Cabinet of Ministers of the Kyrgyz Republic.

This information was analyzed by experts, representatives of law enforcement agencies, and international organizations, represented by EAG Secretariat specialists, allowing a deep threat assessment, as well as improved monitoring of possible threats at the national and transnational levels.

The analysis of terrorist financing threats was mainly based on a wide range of information sources, including operational data, criminal case records, court decisions, international cooperation records, and others.

The following key sources of information were used in conducting a comprehensive assessment of the terrorist financing threat in the Kyrgyz Republic:

1. Strategic documents related to countering terrorism;
2. Results of the EAG Regional Risk Assessment;
3. Reports on financial intelligence unit CFT operations;
4. Internal materials and reports of the State Financial Intelligence Service;
5. Close cooperation with competent authorities, including the Ministry of Internal Affairs, the State Committee for National Security, and the Prosecutor General's Office;
6. FIU's international cooperation, including through the Egmont Group;
7. Requests for mutual legal assistance between states;
8. Data and materials collected from court trials on terrorism and extremism.

Risk assessments reported by the State Financial Intelligence Service include summarized data collected from various sources and with different methods in order to identify and mitigate terrorist financing threats in the Kyrgyz Republic. It includes:

1. Threat categories. Key conclusion from the assessment of threats of terrorism financing is that most of the criminal schemes aimed at financing terrorist organizations in Kyrgyzstan are related to persons involved in armed conflicts abroad, as well as recruitment networks and terrorist propaganda. These persons may be Kyrgyz Republic citizens or foreigners who are associated with active terrorist groups. Threats identified include:

- ***Terrorist organizations and their affiliates*** using financial networks to raise and transfer funds;
- ***Individual terrorists and their accomplices*** relying on self-financing and private donations;
- ***Recruiters and terrorist propagandists*** leveraging digital platforms for fundraising;
- ***Persons involved*** in combat operations abroad receiving funding from abroad.

2. There are several schemes employed to finance terrorist activities, which vary depending on the flow of funds and the method of transfer.

Low-traceability methods are particularly noteworthy:

- Self-financing, i.e. when terrorists use personal funds;
- Private donations through charitable organizations and anonymous crowdfunding platforms;
- Social media and messaging platforms used for fundraising and coordination of payments;
- Money transfer systems are the most common method for transferring funds;
- Cryptocurrencies are a growing threat due to the difficulty of tracking transactions;
- Commercial ventures, where businesses may serve as a front to launder proceeds.

Remarkably, traditional methods such as money transfer systems remain in use alongside newer instruments like e-wallets and bank cards registered with foreign financial institutions.

The presence of multiple terrorist financing channels in Kyrgyzstan poses a threat to both national security and the stability of financial systems. This highlights the urgent need for stricter regulation of illicit financial activities and more expeditious monitoring of suspicious transactions.

3. Purpose of terrorist financing. According to the analysis, money is raised and transferred for a variety of purposes: from training and preparing new fighters to financing terrorist operations and maintaining presence in conflict zones. Main purposes include:

- Training and preparing new fighters for operations in potentially dangerous areas;
- Providing equipment, accommodation, weapons, and other logistical support for combat activities;
- Material support for the upkeep of terrorist groups and their members.

4. Geographic threats and national specifics. Turkiye, Syria, and Afghanistan are among major countries of focus for tackling terrorist financing challenges in Kyrgyzstan. Territories of these countries are used for channeling funds directly into zones of Turkestan[1] and vast nearby areas.

Monitoring systems and available legal cooperation among these countries and their relevant authorities are essential to addressing terrorist threats and disrupting associated flows of funds.

5. Operational countermeasures. To counter the financing of terrorist activities, relevant authorities of the Kyrgyz Republic monitor and analyze suspicious financial transactions. In the reporting period, over 100,000 suspicious transaction reports were processed.

Most flagged transactions involved remote payment systems, with increased attention also given to cryptocurrency transfers, financial flows through social media and messaging platforms, and commercial entities.

6. Legislative initiatives. For a more effective response to terrorist financing, we must:

- Enhance control over digital assets by introducing mechanisms for monitoring cryptocurrency transactions;
- Expand the authority of financial intelligence units, particularly for improving cooperation in international frameworks where the FIU of the Kyrgyz Republic takes part (e.g., EAG, CH FIUs, Egmont Group);
- Improve transparency of charitable foundations through mandatory financial reporting and external audits.

The comprehensive terrorist financing risk assessment in Kyrgyzstan has enabled the identification of key risks requiring increased focus and development of effective combating means. Leveraging technology and international collaboration can significantly improve the ability to track and disrupt cross-border terrorist funding, contributing to peace and security across Central Asia.

[1] Turkestan – historical area within the Central Asian Region until 1920s.

COUNTERING TERRORIST FINANCING AND INFORMATIONAL SUPPORT AMID EMERGING RISKS

In recent years, the financial activities of terrorists have evolved dramatically, introducing new threats that were previously unimaginable. This demonstrates the importance of continuous risk assessment and the incorporation of findings into the operations of law enforcement and supervisory bodies.

DMITRY DANILOV
Head of the General Department of Supervision over Compliance with Federal Laws, Prosecutor General's Office of the Russian Federation

To uphold the rule of law, Prosecutor General's Office of the Russian Federation monitors the compliance with federal laws, including Federal Law On Countering Money Laundering and Terrorism Financing No. 115-FZ dd. August 07, 2001.

According to Subparagraph 11 of Paragraph 47 of the National Security Strategy approved by Presidential Decree No. 400 dd. 07/02/2021[1], preventing offenses related to money laundering and terrorist financing is a priority for prosecutorial oversight. In light of current challenges, the focus is increasingly on the criminal misuse of information and communication technologies, and on preventing radicalization and illegal encroachments among youth.

The Concept of Countering Terrorism in the Russian Federation, as approved by the President, identifies the financing of terrorism and the dissemination of extremist ideologies via the Internet[2] as important factors contributing to the rise of terrorism. Practice confirms that no terrorist act or attack of terrorist fighters can be executed without adequate material support - funding for weapons, training, transport, and other necessities.

Equally, information support is vital for recruitment and propaganda, which serve to maximize the psychological impact of terrorist actions and create widespread insecurity.

International terrorist organizations cannot function without sponsors or digital propaganda. Prosecutors work to eliminate the aforementioned facilitating conditions of terrorist activity.

[1] Corpus of Legislation of the Russian Federation, No. 27 (Part II), Art. 5351 dd. 07/05/2021.

[2] Subparagraphs "d", "f", "g" of Paragraph 2 of the Concept of Countering Terrorism in the Russian Federation approved by the President of Russia on October 05, 2009 (Rossiyskaya Gazeta, No. 198, October 20, 2009).

In recent years, the financial activities of terrorists have undergone significant changes, introducing new threats that were previously unimaginable. This underscores the critical need for risk assessment and the integration of its findings into the practices of law enforcement and supervisory authorities. Prosecutors systemically utilize national assessment of terrorist financing risks and sectoral assessments, prioritizing the most pressing threats and vulnerabilities.

A recent development involves the provision of illegal financial support through legitimate business entities, which were previously attempting to keep distance from criminal activities of particularly anti-social and anti-state nature, like terrorism.

For example, Russian assets belonging to N company, listed by the FFMS for terrorism and extremism involvement, were seized through legal proceedings initiated by the Prosecutor General's Office. The court ordered the transfer of production companies that funded attacks on civilian infrastructure in Russia to state ownership.[3]

Civil liability for terrorists not only acts as a preventive measure but also provides a means to compensate victims of terrorism. For example, in one Russian region affected by terrorist attacks, more than 6.6 billion rubles were allocated to rebuild housing for affected civilians.[4]

However, many terrorists lack sufficient personal assets to offset the damages. In such cases, the state steps in to provide victim support. Following the terrorist attack at Crocus City Hall, regional authorities distributed compensation ranging from 500,000 to 3 million rubles per person, depending on the severity of the harm suffered[5]. These costs are subject to recovery from the assets of the perpetrators and their accomplices.

Modern terrorists increasingly rely on so-called "money mules"—nominal holders of digital payment accounts - which allows them to exploit legitimate financial systems. This includes combining transfers via the Faster Payments System, ATM cash withdrawals, and re-entry of funds into the non-cash circulation. This way of obscuring the identities of real beneficiaries is employed not only by terrorists, but also by conventional financial criminals, especially phone scammers.

The number of crimes committed with the use of information and telecommunication technologies increased by 25% in 2024 compared to the previous year, reaching a total of 765,000 incidents.

This trend significantly elevates the risk that proceeds from cybercrime may be used to finance terrorism. According to the Ministry of Internal Affairs of the Russian Federation, terrorist financing channels increasingly rely on funds from illicit transactions and assets circulating in the shadow economy.[6]

To counter this negative trend and reduce the risks of terrorist financing through cybercrime, all government authorities must intensify their efforts to combat the nominal ownership of financial instruments. Accordingly, prosecutors, in cooperation with the Bank of Russia, the Federal Financial Monitoring Service, and internal affairs authorities, are taking coordinated action to dismantle the use of so-called "money mules". For example, last year prosecutors filed about 9,000 lawsuits to protect the rights of victims of Internet fraud, involving claims exceeding RUB 1.7 billion.[7]

It should be noted that digital space demands a high degree of user vigilance. Failure to adhere to basic digital security practices increases the likelihood of victimization, which in turn raises the risk of individuals becoming complicit in criminal activities. Increasingly, individuals fall into financial distress due to online scams, and are subsequently manipulated by criminals to commit acts of terrorism, such as arson attacks on military commissariats and critical infrastructure.[8]

A recent development involves the provision of illegal financial support through legitimate business entities, which were previously attempting to keep distance from criminal activities of particularly anti-social and anti-state nature, like terrorism

[3] https://www.interfax.ru/russia/969092.
[4] https://t.me/Hinshtein/9471.
[5] https://ria.ru/20240323/vyplaty-1935229112.html.
[6] https://tass.ru/proisshestviya/22679107.
[7] https://tass.ru/obschestvo/23183777.
[8] https://t.me/genprocrf/2916.

Law enforcement agencies have recently observed a rise in fraud schemes structured as Ponzi schemes linked to the financing of illegal armed groups, including through the use of digital currencies[9].

The damage can exceed hundreds of millions of rubles, while the sheer multitude of such Internet projects hinders their effective identification in operational and investigative activities.

To intercept these schemes at the initial stage, the Prosecutor General's Office, in collaboration with the Bank of Russia and the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), works to identify and block web resources that spread information on illegal financial services. Last year alone, 44,000 websites were blocked at our request. Nevertheless, further progress is needed in assessing the criminal liability of scheme organizers and improving typology-based content classification to enhance operational efficiency.

44 thousand

websites were blocked in 2024.

There is growing concern over the involvement of minors in both terrorist and financial crimes. A recent case saw a schoolboy manipulated by cybercriminals into setting fire to a Moscow district administration building[10].

We regularly spot the release of new online games actually disguising the entities that offer income opportunities at the expense of additionally attracted users without proper licensing - such as Potter-Money and Best Fiends, etc. Based on the content, these platforms often target children.

Minors' bank cards are increasingly being used in suspicious financial transactions. In a number of cases, the amounts passing through accounts opened in children's names significantly exceed the combined income of both children and their parents. A review conducted by the Prosecutor General's Office revealed a spike in juvenile financial crime in certain regions of the Russian Federation. According to FFMS reports, these are the same regions that register some of the country's highest levels of suspicious transactions involving minors.

Combined, these facts, in our opinion, indicate the need to strengthen youth prevention measures, including expanding financial literacy programs. The FFMS, the Bank of Russia, and the Ministry of Finance are expected to play an active role, while prosecutor's offices continue to contribute to legal education and awareness-raising among youth.

A crucial element in preventing the spread of extremist ideologies is limiting online access to radical and harmful content.

In 2024, based on the monitoring of Internet space, the Prosecutor General's Office submitted

1,200 requests to Roskomnadzor to restrict access to non-compliant websites, leading to the blocking of more than 75,000 online resources.

There remains a pressing need to hold telecom operators accountable for blocking spoofed traffic. This issue was discussed at the session of the Coordination Meeting of Heads of Law Enforcement Agencies of the Russian Federation held last year. Authorized government agencies have been instructed to prioritize the monitoring and blocking of illegally sold SIM cards, strengthen regulations for identifying telecommunications subscribers, and impose liability on dealers of such technical devices and persons acting on behalf of telecommunications operators[11].

In 2024, more than 1,500 administrative proceedings were initiated under Article 13.2.1 of the Russian Code of Administrative Offenses. These resulted in 530 court rulings and fines totaling RUB 216.5 million.

The Prosecutor General's Office, in close cooperation with the FFMS, continues to apply a risk-based approach in its oversight efforts. This collaboration is regarded as a particularly promising area, with the FFMS providing valuable data to support prosecutorial supervision. Expanding this line of cooperation, including bilateral information exchange, remains a shared goal.

« The Prosecutor General's Office, in collaboration with the Bank of Russia and Roskomnadzor, works to identify and block web resources that spread information on illegal financial services.

[9] https://tass.ru/proisshestviya/22758345.
[10] https://tass.ru/proisshestviya/23000479.
[11] https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=98418092.

PREVENTING SPREAD OF TERRORISM AND EXTREMISM AMONG YOUTH IN REPUBLIC OF TAJIKISTAN

Terrorism and extremism, along with their manifestations - such as criminal terrorist acts, extreme nationalist and separatist movements, and religious extremism - represent highly dangerous socio-political and criminal phenomena. These pose a significant global threat to the security of the world and humanity, constituting a major challenge today.

KHALIM MIRZOALIEV
Director of the Financial Monitoring Department under the National Bank of Tajikistan

The involvement of young people in terrorist or extremist activities is a pressing threat.

Among the most vulnerable to radical influence are young people with their energy, inexperience, and ambition. Youth are the future of any nation, and their engagement is key to building a stable society. Hence, all sectors of society - not just the state - must share in the responsibility of protecting them. Nevertheless, young people are often targeted by terrorist and extremist recruiters who take advantage of their vulnerability, lack of information and striving for self-realization.

Root causes of youth radicalization include social insecurity and economic disparity, young age, influence from the Internet and social media, lack of adequate upbringing in the family, adverse community environments, as well as exposure to political and religious conflicts.

Tajikistan has implemented and continues to pursue various measures to prevent the spread of terrorism and extremism among its youth.

In accordance with the Tajikistan's National Strategy on Countering Terrorism and Extremism 2021-2025, the government has undertaken targeted initiatives to disrupt radicalization pathways. The Strategy is based on a full understanding of the root causes and long-term consequences of extremism and terrorism for the state. Preventing and countering extremism and terrorism requires the commitment and collaborative efforts of government agencies, non-governmental organizations, and civil society.

Thus, this Strategy is based on an integrated approach that combines the efforts of both the government and society.

Furthermore, the government of Tajikistan implements repatriation and reintegration initiatives for women and children returning from war zones, with a number of initiatives aimed at recovering and reintegrating its citizens, particularly families, associated with terrorist groups. Through these programs, over 300 women and children who were trapped in dire circumstances have been gradually repatriated from Syria and Iraq.

The Government of Tajikistan has also adopted a program for 2023–2027 to facilitate the rehabilitation, reintegration, employment, and education of women and children returning from conflict zones. Through this initiative, proactive measures are being implemented to support their return to normal life.

The Department of Financial Monitoring under the National Bank of Tajikistan, in collaboration with law enforcement agencies and other state bodies, is actively working to prevent citizens, particularly young people, from being drawn into terrorist and extremist activities.

The Department has established that more than 50% of the total number of persons listed on the national register of persons associated with terrorism are youths aged 16 to 34. A key focus of the Department's efforts is identifying and disrupting financial flows that may support terrorist and extremist organizations. These actions not only halt the funding of illicit activities but also mitigate the risk of youth involvement in criminal networks.

Young people must be aware of the threats and understand how to counter them. To this end, the Department actively engages with the Youth Council of the national and central banks of CIS countries, educational institutions, public organizations and youth associations, and contributes by delegating speakers and moderators at lectures, trainings, and seminars. Department representatives speak on media platforms to raise awareness among youth about the risks and consequences of engaging in illegal activities. For instance, under the National Financial Inclusion Strategy of the Republic of Tajikistan for 2022-2026, Department's officers jointly organized financial literacy festivals in various cities to raise financial awareness and protect the rights of financial service consumers.

Also, with the support of the International Training and Methodology Center for Financial Monitoring (ITMCFM), we published 500 copies of the guide called "Specifics of National Systems for Combating Money Laundering and Financing of Terrorism (AML/CFT) in Eurasian Region. Vol. 3. Republic of Tajikistan". In collaboration with the Ministry of Education and Science of the Republic of Tajikistan, the majority of these books were distributed to member universities of the International Network Institute and other educational institutions to enhance students' awareness on financial security.

The Department continues to pursue these initiatives to promote national and regional security and looks forward to expanding international partnerships to achieve common goals.

In conclusion, I must note that effective prevention of terrorism and extremism among youth requires a comprehensive approach involving government agencies, educational institutions, civil society, and young people themselves. Promoting critical thinking, financial and legal literacy, and moral responsibility are essential components of a long-term solution.

● **The Experience of the Republic of Tajikistan shows** that consistent efforts to re-integrate citizens, disruption of terrorist financing, and educating young people yield tangible results. However, enduring success depends on expanding international cooperation and adopting best practices.

Thus, preventing the spread of extremist and terrorist ideas among young people is not only the task of government - it is the collective responsibility of society. Only through joint efforts can we create an environment where young people can realize their potential in the service of peace and stability.

CONTRIBUTION OF FADN SITUATION CENTER TO COUNTERING RADICAL IDEAS AND THEIR FINANCING

The Situation Center maintains 24/7 information communication with 89 Russian regions to ensure timely handling of conflict situations. In 2024, the Center identified key threats, including the spread of extremist and terrorist ideologies within ethnic and religious contexts, the promotion of separatism, manifestations of neo-Nazism, and the dissemination of radical interpretations of Islam.

YURY SEDYKH
Senior Analyst of the FADN Situation Center

For a more effective response to destructive external influences, particularly those with characteristics of extremism and terrorism, the President of the Russian Federation instructed to establish the Situation Center of the Federal Agency for Ethnic Affairs of Russia (FADN). Its main purpose is round-the-clock monitoring of the information space and analysis of the key threatening factors in the inter-ethnic and inter-confessional environments.

The main monitoring tool employed is the state information system for monitoring inter-ethnic and inter-confessional relations and for the early prevention of conflicts.

The Situation Center maintains 24/7 information communication with 89 Russian regions to ensure timely handling of conflict situations.

The Situation Center identified a number of key threats in 2024:

The proliferation of extremist and terrorist ideologies within ethnic and religious environments. The dissemination of information intended to undermine inter-ethnic and inter-confessional harmony, including calls for violent overthrow of the constitutional order of the Russian Federation.

The promotion of separatism. Since 2022, foreign-sponsored networks affiliated with the Free Nations of Post-Russia Forum* (designated as a terrorist organization by the Supreme Court of the Russian Federation in 2024) have actively organized online advocating for the division of the Russian Federation into 41 independent states.

In addition, various terrorist groups remain active in Russia, including Ateş*, the Russian Volunteer Corps*, the Freedom of Russia Legion*, the Bashkort Company*, the Karelian Group "Nord"*, and others. These groups engage in information campaigns designed to involve Russian citizens in extremist and terrorist activities and recruit them for taking part in military actions.

Manifestations of neo-Nazism. Amidst the growing number of publications about illegal and anti-social behavior attributed to individuals with migrant backgrounds and with the public outcry surrounding them, there is a rising spread of neo-Nazi ideology in Russian society. The Situation Center has observed a rise in "direct action" incidents targeting migrants.

Also, anti-migrant and anti-Caucasian media channels have emerged, often framing local conflicts involving migrants or individuals from the North Caucasus as ethnic in nature. These publications frequently use inflammatory and biased rhetoric, exacerbating inter-ethnic tensions.

Spread of radical Islam. A significant threat identified is the spread of radical Islam, particularly in the Volga and North Caucasus regions and among migrant communities.

In 2024, networks distributing radical Islamist literature were uncovered by the Situation Center, primarily in the Volga region, the North Caucasus, and Crimea. These networks were linked to extremist preachers and international terrorist organizations based abroad.

Supporters of this organization consistently raise funds to support its activities. In early 2022, members of extremist and terrorist groups frequently collected money using personal bank cards issued in Russia. However, as authorities intensified efforts to counter the financing of such activities, the process has grown more complex due to the increasing use of cryptocurrency wallets. Offenders leverage these wallets in an attempt to maintain anonymity and evade detection by law enforcement agencies.

One notable case involves Mikhail Oreshnikov, a neo-Nazi and founder of the terrorist group Nukhrat Palhar Party Silver Bulgaria*, who created his own cryptocurrency to fund separatist activities in the Chuvash Republic.

The Situation Center regularly transfers intelligence on funding mechanisms to law enforcement agencies and the Federal Financial Monitoring Service for follow-up response measures.

To enhance efforts in identifying and neutralizing threats posed by extremist public associations and influencers, and to provide an objective assessment of the level of social tensions in the North Caucasus Federal District, the Interregional Department of the FADN in the North Caucasus Federal District, the Republic of Crimea, and the city of Sevastopol has initiated cooperation with the FFMS Interregional Office (FFMS IO) in that region.

In the first quarter of 2024, joint working meetings with FFMS IO leadership were held to establish a cooperative framework.

As part of interagency cooperation, 48 reports detailing key developments in inter-ethnic and inter-religious relations in the North Caucasus Federal District have been submitted to the FFMS IO since February 2024. These materials were obtained from the State information system for monitoring inter-ethnic and inter-confessional relations and early prevention of conflicts. On average, one report summarizes 100 relevant publications.

Furthermore, the FFMS IO for the North Caucasus Federal District receives weekly analytical briefings on short-term and long-term forecasts regarding potential focuses of inter-ethnic tension.

The established interaction protocol has enabled timely mutual notification regarding potential ethnic and religious escalations and attempts to raise funds for financing extremist and terrorist activities. It also ensures an appropriate level of situation monitoring.

Based on this intelligence, the Interagency Commission for Countering the Financing of Terrorism froze the assets of 6 members of the Ingush Independence Committee[1] (IIC) residing abroad. Also, Ingush journalist Magomed Toriev, an IIC member, was added to the Ministry of Justice's List of Foreign Agents as of November 15, 2024.

* Designated as terrorist, activities banned in the Russian Federation.

[1] Listed by the Ministry of Justice of the Russian Federation in the List of Foreign Agents and International Organizations whose activities deemed undesirable in the Russian Federation.

TERRORISM IN NORTH CAUCASUS: FFMS NCFD INTERREGIONAL OFFICE EXPERIENCE

Combating terrorism in the North Caucasus remains a top priority for government agencies tasked with detecting, preventing, and investigating related crimes. The evolving security landscape and previously unknown typologies necessitates the development of new strategies for identifying individuals involved in terrorist activities.

GRIGORY TARANENKO
Representative of the Interregional Office of the Federal Financial Monitoring Service for the North Caucasus Federal District

On June 23, 2024, an armed group launched coordinated attacks on religious sites in Makhachkala and Derbent in the Republic of Dagestan. They targeted Orthodox churches and Jewish synagogues. Their actions resulted in 46 casualties, including 17 fatalities among clergy and law enforcement personnel.

The attackers were identified by security forces prior to arrival of special units at the crime scenes and were subsequently neutralized during a counter-terrorist operation conducted the same evening.

Immediately following the incident, the Interregional Office of the FFMS in the North Caucasus Federal District coordinated operational measures with the Federal Security Service units in the region and district. Under the direction of the FFMS Department for Countering Terrorist Financing, efforts to trace the attackers' financial and other connections began even before the counter-terrorist operation concluded.

Post-operation, the priority shifted to identifying accomplices. Within three days, a comprehensive financial investigation tackled 50 individuals connected to the perpetrators and over 17,000 affiliated entities and counterparts.

The variety of examination activities uncovered traces of terrorist financing through bank accounts and cards, cash, and informal transfer systems that do not require opening an account.

Furthermore, it also revealed significant connections between the attackers and certain municipal authorities.

The identification of terrorist links to certain local officials was taken into account while planning broader efforts to detect individuals connected with terrorist activities.

These individuals did not meet the previously established objective, behavioral, or financial criteria used to identify terrorists and saboteurs. Consequently, the action plan for identifying individuals vulnerable to terrorist recruitment has been adjusted in line with the actual operational environment.

Moreover, given the extraordinary nature of the recent incident, a decision was made to take additional proactive measures to identify persons involved in terrorist activity and those who supported the terrorists of the attack in Dagestan.

An extensive examining was conducted, focusing on approximately 25,000 residents of one district in Dagestan and broader at-risk contingent of the Republic residents.

The identification procedure involved a detailed analysis of individuals associated with terrorism related crimes, residents of specific areas and the Republic as a whole, and financial transactions marked with anti-money laundering and counter-financing of terrorism AML/CFT codes.

Through cross-analysis of data from the Federal Financial Monitoring Service's (FFMS) databases, and by applying specific objective, behavioral, and financial indicators, investigators identified financial connections between the attackers and radical Islamic preachers based abroad. These included individuals such as Abu Umar Sasitlinsky, Abdullah Kosteksky, Ali Charinsky, and others known for their involvement in terrorist and extremist activities. According to operational intelligence, these individuals are covertly recruiting youth in the Republic to join "sleeper cells."

Subsequent investigations examined the financial activity of more than 1,000 residents of Dagestan classified as high-risk contingent. Notably, a significant drop in financial activity - nearly fivefold - was recorded among this group in the period leading up to the terrorist attack.

In conclusion, I would like to note that these enhanced identification measures proved effective, yielding tangible results that contributed to the stabilization of the security situation in the region.

As a result of the findings provided by the Interregional Office (IO), two criminal cases were initiated against five individuals for preparing terrorist acts, and one case was opened for money laundering of criminal proceeds.

Importantly, intelligence regarding one of the attackers' associates had been submitted to law enforcement in advance. Information concerning the networks of terrorists residing or operating in other Russian regions was swiftly communicated to the respective FFMS territorial offices.

Following the decision of the Interagency Commission for Combating the Financing of Terrorism, measures were taken to freeze the assets of two persons associated with the attackers.

The Interregional Office of FFMS provided materials that allowed to dismantle an emerging "sleeper cell" of an international terrorist organization in the Republic of Dagestan.

A key priority moving forward is to implement integrated profiling initiatives targeting young people in the Republic and the district. These efforts aim to reduce the risk of youth involvement in terrorist, extremist, or other destabilizing activities.

CYBER TERRORISM: EMERGING CHALLENGES AND RESPONSES

NCCTI'S APPROACH TO PREVENTING MISPERCEPTION-BASED DIGITAL MARGINALIZATION OF YOUTH

In the context of modern digital society, where information is widely and instantly disseminated, cultivating well-informed and socially responsible youth has become a pressing concern. Educational efforts aim to shape a constructive civic identity. In this regard, education - especially its preventative role - serves as a critical tool for social integration, counteracting marginalization. During marginalization, individuals may discard learned norms and values, distancing themselves from societal institutions and opportunities.

SERGEY CHURILOV
Head of NCCTI NRI Spetsvuzavtomatika

The most dangerous form of marginalization in the modern information space is digital marginalization, i.e. a person's transition to a borderline state, marked by blurring civic identity and a loss of understanding of social norms and values. The perception of the digital space as supposedly under-regulated by the current legislation can shape the opinion that one may commit unlawful acts and not suffer adequate consequences. In other words, digital marginalization as a particular form of marginalization becomes a link in the process of radicalization potentially escalating to extremist or terrorist behavior.

I must note that the most difficult problem is countering the recruiters' activities in the digital space. Importantly, the recruiters mainly target vulnerable groups, including youth, individuals in distress, those discontented with current sociopolitical conditions, former combatants, and persons affected by conflict-related loss. Speaking of the level of education, the National Center for Countering Terrorism and Extremism in the Information Space (NCCTI) research conducted from 2021 to 2024 indicates that individuals with secondary or vocational education are most commonly involved in unlawful acts.

In addition to direct criminal participation, there is an urgent need to protect internet users - especially children and adolescents - from online fraud. Prevention experts must remain vigilant and informed about the latest fraudulent schemes:

- Giveaways by famous bloggers. Fraudsters create fake social media profiles impersonating well-known bloggers and announce fake giveaways (for example, video game consoles or in-game currency). To claim their "prize", supposed winners are asked to pay for delivery and provide personal information to a "manager," who is, in fact, a scammer. This allows the fraudster to gain access to the user's personal accounts.

- Teacher's call scam. With the use of deepfake technology, scammers

fake the voices of a child's teacher. They contact students, instructing them to update their student profiles on the Sferum app, and trick them into revealing a code received via text message. This code is a verification password granting access to the Public Services Portal and sensitive personal data.

- Like and earn scheme. Scammers lure children with advertisement for seemingly quick and easy jobs. They offer a generous reward for a few likes on social media. Once the job is done, they request the user's bank details for "payment," thereby gaining access to personal financial information.

As part of ongoing preventive work efforts, included in the general educational activities, it is essential to align and accomplish the following tasks:

- Equip young individuals with the tools to resist digital manipulation and recruitment tactics, while cultivating critical thinking skills.

- Debunk myths and misconceptions that portray terrorist or extremist activities in a positive light, emphasizing the ineffectiveness of such methods in addressing socio-political grievances.

- Increase legal literacy in anti-terrorism and anti-extremism legislation, as well as other legal areas that could be of practical use, e.g. personal data protection.

- Dispel historically inaccurate narratives circulating online that aim to erode civic identity and foster anti-state sentiments.

Main goal of prevention is to ensure consistent and sustained socialization of all residents of the country, particularly those most vulnerable to harmful influences (risk groups). Let's not forget that one of the factors of digital marginalization is a simple ignorance of how to use modern information resources. That is why fostering media literacy and digital competence is essential for safeguarding individual users and strengthening the integrity of the information environment.

Over the years, the NCCTI has accumulated substantial experience in preventing the spread of digital marginalization and the resulting involvement of young people in illegal activities:

- Comprehensive Prevention Toolkit: Includes scenarios, methodological guides, and educational resources. Notably, four compendiums of both general and targeted prevention scenarios were published between 2022-2024.

- Specialist Training Programs: Designed not only to teach preventive measures but also to foster meaningful, balanced engagement with young people. For instance, the School of Lecturer national intensive training initiative, launched in 2024, has been held in five regions of Russia, involving 359 participants. Expansion to at least nine additional regions is planned for 2025.

- Youth-Oriented Outreach materials: Includes informational cards and videos tailored for accessibility. These resources are produced under three major projects: Nationwide Content Factory Parallels, a national initiative to build a youth media community; Peremenka (Recess), an online show where schoolchildren interview experts; and the Answers nationwide online show, where experts in various fields answer youth-submitted questions.

Thus, the complexity of the raised problems determines the need for a multidimensional solution toolkit. Qualified and continuously advancing specialists, efficient systematic work, up-to-date tools consisting of scenarios, formats and methods of work, ongoing updating of the information space with constructive content will significantly reduce digital marginalization and, as a result, prevent the involvement of citizens in illegal activities to the maximum extent possible.

DIGITAL TERRORISM: HOW MODERN TECHNOLOGY FUELS EXTREMISM AND TERRORIST FINANCING

AHMED BARAKA
Egyptian financial intelligence unit representative

Modern technologies have not only changed our lives, but also created new challenges in the fight against terrorism. Criminal groups are adapting to the digital environment, using social media for recruitment, cryptocurrency for funding, and cyberattacks to destabilize societies. In order to counter these phenomena, coordinated work of national structures and global cooperation between countries are necessary.

SOCIAL MEDIA: THE DIGITAL BATTLEFIELD FOR RADICALIZATION AND RECRUITMENT

Social media platforms, originally designed to connect people and foster global dialogue, have become powerful tools for terrorist organizations. These groups exploit social networks to spread propaganda, glorify violence, and recruit vulnerable individuals.

How Social Media is Used for Radicalization ?

- Terrorist groups create high-quality propaganda videos, often mimicking Hollywood-style production techniques, to appeal to young and impressionable audiences. These videos, along with radical messages, are shared in encrypted chat groups and closed forums, making detection challenging for authorities.

- For example, ISIS* successfully recruited thousands of foreign fighters through its sophisticated online presence. It used emotionally charged narratives—portraying itself as a protector of oppressed Muslims—to lure recruits from Europe, North America, and Asia. The group even gamified its recruitment efforts, offering rewards and recognition to those who successfully brought in new members.

- A study from George Washington University reveals that 70% of people who joined terrorist groups like ISIS* were exposed to radical content on the internet via social media platforms. These platforms have become ideal tools for spreading extremist messages and recruiting vulnerable individuals.

The Role of Encrypted Messaging Apps

While mainstream platforms have cracked down on terrorist content, extremist groups have moved to encrypted messaging apps with private channels, where members can communicate securely, coordinate attacks, and share bomb-making instructions[1].

CRYPTOCURRENCY AND ONLINE FINANCIAL TRANSACTIONS: THE HIDDEN FUNDING SOURCE FOR TERRORISM

Traditional financial systems have long been monitored to prevent money laundering and terrorist financing, but cryptocurrencies have provided extremist groups with a new, untraceable means of funding.

[1] Source: https://www.un.org/securitycouncil/ctc.

Why Cryptocurrencies Are Attractive to Terrorists?

- Anonymity: Unlike bank transfers, cryptocurrency transactions can be conducted without revealing personal identities.
- Decentralization: With no central authority regulating transactions, it becomes difficult for governments to freeze assets.
- Borderless Transactions: Cryptocurrencies enable international money transfers without the need for banks, making it easier to fund operations globally.

How Terrorists Use Cryptocurrencies

Terrorist groups raise funds through various means:

- Crowdfunding on the Dark Web: Extremist groups create anonymous fundraising campaigns disguised as humanitarian causes.
- Hiding Transactions in Blockchain Mixers: These services break up transactions into smaller pieces, making it nearly impossible to trace the original source.
- Using Bitcoin for Ransom Payments: Ransomware attacks, often linked to terrorist organizations, demand payment in Bitcoin to finance further operations.

In 2020, the U.S. Department of Justice seized millions in cryptocurrency linked to Al-Qaeda* and ISIS*, proving that digital currencies have become a critical tool for terrorist financing.[2]

CROWDFUNDING AND TERRORISM FINANCING

What is crowdfunding?

Crowdfunding is the practice of soliciting contributions from a large number of people, especially from the online community and usually in smaller amounts, to support an idea, project or business venture.

How crowdfunding could be used In terrorism financing

There are four main methods that terrorists and violent extremists use to raise funds through crowdfunding.

1. Abuse of humanitarian, charitable and non-profit causes which can act as a front to raise funds for terrorism.
2. Dedicated crowdfunding platforms or websites which, given the volume and variety of activity, makes it difficult to detect illicit activity.
3. Social media platforms and messaging apps to allow extremists to amplify their messages and lead users to specific fundraising causes.
4. Interaction of crowdfunding with virtual assets, including the use of privacy coins and anonymity enhancing services such as tumblers and mixers.

In practice, terrorists often use a combination of techniques and methods. For example, they may establish a fundraising campaign on a dedicated crowdfunding platform, share the campaign on social media, and request payment in virtual assets.

Most crowdfunding is legitimate. Unfortunately, crowdfunding, and in particular donations-based crowdfunding is also being misused to raise funds to finance terrorism.[3]

THE ROLE OF TECHNOLOGY IN PLANNING AND EXECUTING ATTACKS

Terrorist groups no longer rely solely on traditional methods of attack. Instead, they use modern technology to plan and carry out operations with unprecedented precision.

The Use of Drones in Terrorist Attacks

Drones, originally developed for commercial and military use, have been repurposed by terrorists for surveillance, smuggling, and even direct attacks. Groups like ISIS* have modified consumer drones to carry explosive devices, turning them into remote-controlled weapons. In conflict zones like Syria and Iraq, drone attacks have become a deadly and unpredictable threat.

Cyberterrorism: Attacking Critical Infrastructure

Instead of planting physical bombs, some terrorist groups now seek to disrupt nations through cyberattacks. By hacking into power grids, financial institutions, and government networks, terrorists can cause widespread chaos without ever stepping onto a battlefield.

[2] Source: https://www.fatf-gafi.org/publications/methodsandtrends/.

[3] Source: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html.

The "WannaCry" attack in 2017 affected 150 countries:

In May 2017, the WannaCry ransomware cyberattack affected 150 countries worldwide. The attack targeted critical sectors such as hospitals, banks, and government agencies, causing massive disruption. While the attack was not directly linked to terrorism, it raised concerns about the potential use of such attacks by terrorist groups in the future[4].

The Danger of AI-Generated Deepfakes

Another emerging threat is the use of deepfake technology—AI-generated videos that can manipulate reality. Terrorist organizations could use deepfakes to create fake speeches from world leaders, inciting violence and mass panic. The ability to fabricate convincing video evidence poses a major challenge for intelligence agencies.[5]

STRATEGIES TO COMBAT DIGITAL TERRORISM

Governments, tech companies, and international organizations are implementing measures to counter the growing threat of digital terrorism. Some of the most effective strategies include:

1. **Strengthening Cybersecurity Measures.** Governments are investing in advanced AI-driven surveillance tools to detect and remove extremist content before it spreads. Machine learning algorithms can analyze vast amounts of data to identify radicalization patterns.

2. **Regulating Cryptocurrencies and Financial Transactions.** Financial regulators are pushing for stricter Know Your Customer (KYC) and Anti-Money Laundering (AML) policies in the cryptocurrency space. Major exchanges are now required to report suspicious transactions, making it harder for terrorists to move funds anonymously.

3. **Enhancing International Cooperation.** Since terrorism is a global issue, intelligence-sharing between nations is essential. Organizations like INTERPOL and Europol are collaborating to track digital footprints left by terrorists and dismantle their networks.

4. **Public Awareness and Counter-Radicalization Programs.** Preventing radicalization before it begins is crucial. Governments are launching counter-narrative campaigns, using former extremists to speak out against radical ideologies. Social media companies are also partnering with authorities to promote positive content that counters extremist messaging.

In a groundbreaking effort, Google's Jigsaw Initiative has developed an AI system that redirects users searching for extremist content to anti-radicalization resources, effectively breaking the cycle of online radicalization.[6]

CONCLUSION

While technology has revolutionized our way of life, it has also created new challenges in the fight against terrorism. Extremist groups have adapted to the digital landscape, using social media for recruitment, cryptocurrencies for funding, and cyberattacks to destabilize societies. However, through a combination of advanced security measures, global cooperation, and public awareness, authorities can counter these threats and ensure that technology serves as a force for good rather than a tool for destruction.

The battle against digital terrorism is ongoing, but with the right strategies, we can disrupt extremist networks and protect the digital world from being exploited by those who seek to harm it.

* Recognised as terrorist, its activity is banned on the territory of the Russian Federation

[4] Source: https://www.csoonline.com/ (Cybersecurity Reports).
[5] Source: https://www.nato.int/cps/en/natolive/topics_77646.htm.
[6] Source: https://www.interpol.int/en/Crimes/Terrorism.

PROPAGANDA OF TERRORISM ON INTERNET IN THE CIS COUNTRIES. RESPONSE MEASURES

This article reviews the evolving methods of propaganda used by terrorist organizations within CIS member states, facilitated by advancements in information and communication technologies. It focuses on the effectiveness of these propaganda strategies in recruiting new adherents and outlines countermeasures.

GENRIKH MELIKYAN
Group Leader of the Anti-Terrorist Center of CIS member states

There is general agreement that the most dangerous terrorist threats in the modern world stem from the integration of information and telecommunication technologies with traditional terrorist tactics. These include recruiting new members, training for sabotage, merging with organized crime networks, and expanding both domestic and foreign funding sources. An increased public danger is the return to the countries of origin of terrorist fighters who have taken part in operations of international terrorist organizations abroad.

CIS ATC pays considerable attention to the spread of terrorist and extremist content on the Internet and its use in so-called information wars.

Combating terrorism and extremism is not only about timely detection and suppression of terrorist and extremist acts. Equally important is to counter the crimes that provide an "infrastructure" for terrorism and extremism. This includes involvement in terrorist and extremist organizations, their financing and other material support, and the dissemination of terrorist and extremist propaganda. Experts note the phenomenon of "self-recruitment," where individuals radicalize through online propaganda and voluntarily seek contact with extremist and terrorist structures.

The efficiency of timely counteraction is significantly hindered by the fact that up to 90% of extremist web resources are physically located outside the CIS territory. To put it plainly, an open information war is being waged against both Russia and our partner states, and the radicalization of citizens is in many ways a direct result of external influence. While the Islamic State* remains a major actor, other groups also contribute significantly to this threat landscape.

Recruitment through social networks is often targeted at citizens of Central Asian states who immigrate to other countries, including Russia, to work. Security and intelligence services across the CIS are working together to prevent such recruitment and to track down persons involved in terrorist and extremist activities who attempt to evade justice by crossing borders within the CIS.

Today, extremism, terrorism - particularly political terrorism cloaked in religious rhetoric - and destructive psychological manipulation can be recognized as interconnected phenomena comprising a unified sociological concept. In fact, the potential of destructive activity continues to grow, increasingly serving as a highly effective tool for disrupting the internal order of entire states and even regions. For instance, Hizb ut-Tahrir* is a banned religious-political organization which ideological objective is to dismantle

the existing constitutional order and replace it with a political-religious regime rooted in political Islam. The organization not only rejects secular authorities, but also disavows official religious institutions. Its recruiters operate in mosques, religious and secular educational institutions, and in densely populated areas inhabited by migrant workers - primarily citizens of Central Asian states of the CIS.

The term "information war" is directly derived from the concept of propaganda, which by now has acquired a negative connotation and is less frequently used. New psychological manipulation techniques regularly supplement the traditional propaganda techniques. In order to attract new members, extremist and terrorist organizations make extensive use of special manipulative techniques at every stage of recruitment. These groups often utilize "in-house" psychologists to recruit and train individuals for either immediate terrorist action or long-term covert operations.

The activities of international terrorist and extremist organizations are heavily connected to the modern information wars, which, in turn, are an integral element of the so-called "hybrid wars". These strategies aim to politically destabilize states, undermine national sovereignty, and alter constitutional systems. As a result, this challenge has escalated into a core national security issue.

Therefore, the structure and scope of information countermeasures in combating terrorism and extremism are radically changing, too. Both the state and the private sector share the responsibility for developing technologies and algorithms for the timely detection, mitigation, and elimination of such threats, including their implementation.

In this context, certain areas of international anti-terrorist cooperation, especially those proven effective within CIS member states, require renewed emphasis.

Policy frameworks of the CIS member states on combating terrorism and extremism direct the operations of security bodies, intelligence services, and law enforcement agencies particularly in safeguarding information security. All CIS member states recognize that protecting the information and communication space is a vital component of national security and information sovereignty. This shared understanding underpins a critical area of collaboration among the security agencies and special services of the CIS member states.

Experts urge us to abandon the narrow, so-called technocratic approach, whereby the very problem of information security is artificially narrowed down to the task of information protection.

Predictably, information security proved to be connected with the practice of so-called mental wars unfolding in the information field nowadays. It is undeniable that Russia and other CIS countries are primary targets of these operations.

The Russian media is not only at the forefront of the information war - it is, in many respects, on the battlefield's front line.

We fully recognize the importance of the CIS states' media policy. The informational dimension of the military agencies' work is equally important. Moreover, for security services and law enforcement across the region, information counteraction has become a routine and essential aspect of maintaining national security and combating terrorism and extremism.

A qualitative analysis of contemporary information warfare tactics has identified several challenges requiring further attention. Chief among these are issues related to the import substitution of software and specific methodologies for online information campaigns in support of combating terrorism and violent extremism. There is also an urgent need to unify methodological approaches to information campaigns in ways that are immediately applicable in practice. Moreover, additional training in information conflict management is needed for decision-makers at national, and regional (both public and corporate) levels.

Experts propose to address the following tasks:

1. Identifying and discussing applied scientific and technical foundations, innovations, and practices for detecting, monitoring, analyzing, and implementing actions for information-psychological counteraction on the Internet.
2. Pinpointing unresolved applied challenges within this field.
3. Building a pool of interdisciplinary teams dedicated to developing methodologies and technologies for information-psychological war on the Internet.
4. Compiling and systematizing the development of software tools and tactical approaches to be used in both general and specialized online counter-propaganda efforts against terrorism and extremism.

Furthermore, it seems reasonable to conduct applied research and develop practical solutions addressing the most urgent challenges, including:

- Structural and behavioral analysis of social media platforms for identifying terrorist threats;
- Utilization of social media big data to uncover propaganda networks and predict related events;
- Development of technologies for analyzing databases retrieved from the dark web containing information on individuals and entities;
- Formulation of methods for launching and countering information campaigns;
- Detection of astroturfing through group behavior analysis and content authenticity assessments;
- Analysis of the role of gamer communities in the dissemination and counteraction of information warfare strategies, etc.

Such initiatives usually involve invited academic experts who specialize in specific aspects of information warfare and information security in general.

The experience gained through cooperation between security, special services, and law enforcement agencies of the CIS member states in preventing terrorist attacks with the use of information and communication technologies allows us to draw important conclusions:

1. Modern threats demand not only a robust defense-in-depth approach but also implementation of proactive strategies at both the strategic and operational levels. Foundational to this approach are national and international information security doctrines, many of which are already in place and successfully implemented across the CIS.
2. With the advancement of modern communication technologies, regional and national initiatives - as well as special programs promoting cooperation in countering terrorist and extremist organizations - have the greatest actual potential.
3. In the context of regional cooperation, specific operational tasks - such as developing methods to identify and combat cyber threats - can be effectively achieved. This includes fostering collaboration not only across national information and communication systems but also among the specialized units responsible for the overall security.
4. CIS member states' competent authorities unanimously emphasize the need to enhance technological capacities for identifying and suppressing terrorism-related content on social media. They also call for IT companies to establish clear protocols for detecting and removing terrorist and extremist materials. In today's security climate, key national and collective security challenges must be addressed through international cooperation. The fight against terrorism and extremism is not an exception and, moreover, exemplifies an area where most effective, coordinated management decisions are worked out.

* Designated as terrorist, activities banned in the Russian Federation.

STUDENT SHIELD: TOGETHER AGAINST TERROR

The CIS ATC and the Moscow State Linguistic University organized the Fifth International Contest of Student Initiatives in Countering the Terrorist Ideology - Student Shield 2025 - in the first half of 2025.

An international jury will evaluate submissions in four categories.

The competition is open to young people under the age of 30. Applications must be submitted by April 30, 2025.

More details

YOUNG PROFESSIONALS TRIBUNE

COOPERATION FOR THE BENEFIT OF INTERNATIONAL SECURITY

The issue of security bears on the world order and the future of humanity. Global security hinges on the collective efforts of nations to address threats that exceed their sovereignty. While some of these threats require collective action, all states have unilateral privileges to act in their national interest within the framework of international law. States place great value on sovereignty. However, when it is used as a weapon, it often becomes an obstacle to meaningful action.

AMIN RAOUFI
Ph.D. Student in Public International Law at University of Tehran

In an increasingly interconnected world, security is guaranteed through cooperation. Thus, it is essential to ensure that cooperation is fully consistent with the rule of law. In fact, cooperation, through its positive practices, becomes a force for good, instead of allowing the nation-state to default into chaos. In this regard, cooperation between subjects of international law emerges not only as a strategic choice but also as a necessary means to ensure peace, security and stability at the regional and international levels respectively.

Internationally, the United Nations (UN), as a comprehensive international entity, plays a remarkable role in maintaining international peace and security. It discharges its duty through international cooperation using diplomacy and mediation, as well as countering terrorism in all its forms. Regarding the latter, the codification of international instruments against international terrorism within the framework of the UN system explicitly reflects the prominence of combatting terrorist activities for the international community. As one of the most experienced entities in the field of tackling organized crimes, the UN has also addressed money laundering as one of the main causes of the financial instability of countries. Besides relevant resolutions adopted by the General Assembly and Security Council, the UN fulfills its mandate, among others, through the Global Program against Money Laundering (GPML). In particular, this initiative has been tasked to provide technical assistance to Member States to combat money laundering and the financing of terrorism in accordance with UN related instruments and internationally accepted standards. Herewith, the UN aims to provide necessary tools to countries and strengthen their capacity to effectively conduct their duties in the field of anti-money laundering and countering the financing of terrorism (AML/CFT).

As financial crimes are rapidly growing, the international community perceived the desperate need for a specialized policy-making body to appear as a backbone of the AML/CFT efforts across the world. The Financial Action Task Force (FATF) as an international standard-setter in the sphere of money laundering and terrorist financing, carries out its duties to guide nations in crafting their AML/CFT frameworks and revising

related laws and regulations as well. Among others, Recommendation 40 affirms that "countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing." As international cooperation becomes paramount, the FATF highlights its significance whether through the exchange of information with foreign counterpart FIUs, mutual legal assistance and the conclusion of bilateral or multilateral agreements. It should be noted that all mechanisms facilitating swift exchange of information, on the one hand, shall be arranged in accordance with national laws and regulations of States involved in the process and on the other hand, shall ensure that criminals cannot exploit jurisdictional gaps to reach their ends. Moreover, sharing best practices and strategies fosters effective role-making in combating financial crimes.

Aside from the international level, the promotion of regional cooperation also has certain benefits. Given the nature of money laundering and the financing of terrorism, solid regional cooperation is the key to effective AML/CFT activities. As an indispensable element for an effective AML/CFT regime, regional arrangements gather officials from the region to discuss their specific concerns to better overcome the very complex AML/CFT issues. The significance of regional arrangements has been stipulated in the 8th chapter of the UN Charter. By virtue of this chapter, the UN Member States have been called upon to enter into such arrangements and deal with matters relating to the maintenance of international peace and security as are appropriate for regional action, provided that such arrangements or agencies and their activities are consistent with the purposes and principles of the UN. Taking into account the significant impact of regional cooperation to achieve international security and in line with the abovementioned purposes and principles, the FATF-Style Regional Bodies (FSRBs) constitute an extensive network to actively participate in combating money laundering and terrorist financing. Likewise, the FSRBs oversee the AML/CFT efforts all over the world and support the implementation of AML/CFT international standards. Deeply recognizing their concern for maintaining economic security in the region, the FSRBs seek efficacious means to threats to the financial systems in regional initiatives. Whereas financial crimes, on a large scale, could have devastating consequences for millions of people and threaten global economic integration, regional initiatives can reinforce economic and financial security aligned with national strategies and priorities. As a result, comprehensive regional approaches in the security sphere could remarkably lead to safeguarding international security.

Hence, we should reaffirm that the interconnected nature of modern threats necessitates collective action. Accordingly, along with other subjects of international law, international and regional organizations have an eminent responsibility. In this regard, the region is an intermediate actor that undertakes tasks determined at the international level. To put it more clearly, regional initiatives are mainly aimed to contributing at the international system to build resilient systems and foster stability. They can bridge the gap between national interests and global objectives and ensure international security. Consequently, global security is not the duty of a single nation or entity but a collective imperative demanding sustained cooperation. While challenges persist, cooperation is the only way to solve problems of the international community and can yield transformative outcomes. In an era defined by both risk and interconnection, the choice is to abide by collaboration.

TERRORIST AND EXTREMIST LISTS AS EFFECTIVE TOOL AGAINST DESTRUCTIVE ACTIVITY

Extremism (from the Latin extremus, meaning "outermost") and terrorism (from the Latin terror, meaning "fear") are the most dangerous forms of destructive behavior in society. These activities are typically characterized by violence, aggression, incitement to hatred on various grounds, etc. These phenomena pose a significant threat to constitutional order, public safety, and the rule of law. This is why combating extremism and terrorism is one of the key goals of law enforcement agencies worldwide.

GERMAN LYUBATUROV
Representative of the Interregional Office of the Federal Financial Monitoring Service for the Central Federal District

The Russian Federation, having faced severe terrorist and extremist threats since the beginning of the 21st century, has been actively developing and improving counter-measures, particularly targeting the financial infrastructure that supports such activities. Important elements of this counteraction are regulation, international cooperation, as well as the use of specialized institutions and instruments designed to monitor and disrupt the terrorists' and extremists' financial flows.

One of the primary tools in this context is the maintenance of terrorist and extremist lists. Figure 2 illustrates the structure and implementation in the Russian Federation of lists of organizations, individuals, and materials to counter extremist and/or terrorist activities.

Each list concerns different aspects of monitoring and countering terrorist and extremist activities, providing the respective authorities with tools to ensure security and compliance with Russian Federation law.

For example, the List of Public Associations and Religious Organizations Subject to Enforceable Court Decisions on Liquidation or Prohibition ensures that any group declared illegal by the courts is dismantled. Furthermore, any form of collaboration with and support of the entities on this list is deemed criminal.

The Federal List of Extremist Materials aims to restrict the dissemination of content deemed to pose significant psychological or moral harm to the public.

It is important to note what distinguishes this list from the List of Public Associations and Religious Organizations Subject to an Enforceable Court Decision on Liquidation or Prohibition and the List of Organizations and Individuals Known to be Involved in Extremist or Terrorist Activities, compiled by the Federal Financial Monitoring Service (FFMS) (further referred to as the FFMS List of Terrorists and Extremists).

Unlike the List of Public Associations and Religious Organizations Subject to an Enforceable Court Decision on Liquidation or Prohibition and the FFMS List of Terrorists and Extremists, the Federal List of Extremist Materials includes books, leaflets, articles, brochures, and newspaper issues deemed extremist. It does not identify the authors, as the real creators, beneficiaries and distributors are often difficult to trace. As of February 2025, this list comprised 5,456 entries.

Another tool for curbing destructive activities in the Russian Federation is the List of Foreign Agents and International Organizations Whose Activities Are Recognized as Undesirable in the Russian Federation.

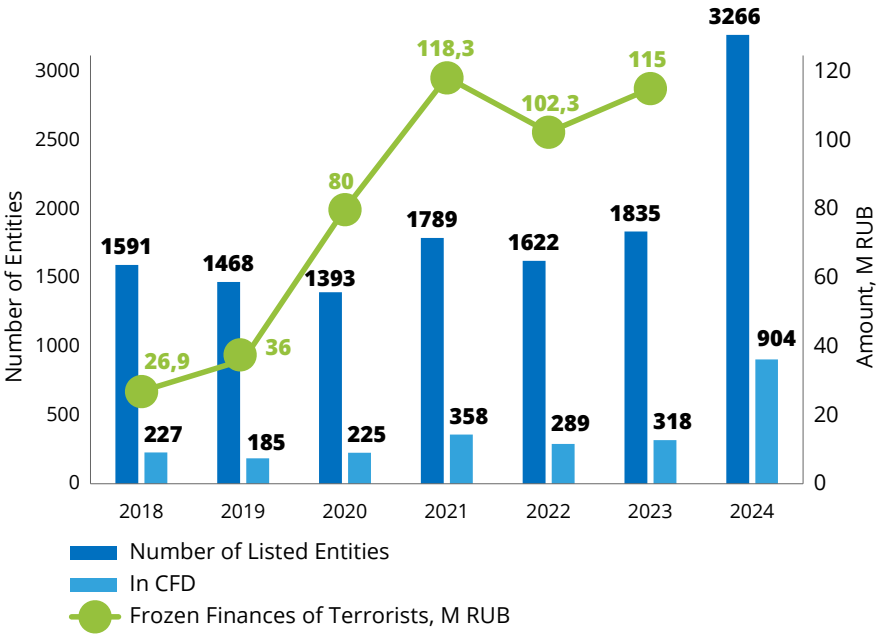
This list includes only foreign and international non-governmental organizations that are posing threats to the constitutional order, defense, or national security through their activities.

The major differences with the above lists are associated with the fact that this list targets foreign-based entities and includes those suspected of engaging in activities contrary to Russian national interests, without necessarily having been subject to legal proceedings in the Russian Federation.

The existence of such a list underscores the international dimension of national security and enables effective control over foreign influence on domestic policy.

As indicated by the data above, over the past five years, the FFMS list has steadily grown in number, driven by the rising number of registered terrorist and extremist crimes in the Russian Federation (Fig. 1).

Figure 1. Statistical Data of FFMS's Terrorist and Extremist List



The distinctions between an extremist organization and an undesirable organization primarily relate to the nature of their activities and the measures that may be applied against them.

The key difference lies in the fact that an extremist organization is defined by its radical ideology and often poses a direct security threat, whereas an undesirable organization may be deemed adverse to national interests due to a range of activities that are not necessarily linked to extremism.

When reviewing one of the core tools of the FFMS — The List of Terrorists and Extremists – we must study its characteristics.

This list is used mainly for rapid response to emerging risks and threats, as it lists entities and individuals based on intelligence and risk assessment, even prior to formal court rulings. This allows authorities to act quickly without engaging in formal judicial proceedings which may be time consuming.

The grounds for inclusion of individuals and entities in the FFMS list are established under Part 2.1 Art. 6 of the Federal Law On Countering Money Laundering and Terrorism Financing No. 115.

The FFMS's Terrorist and Extremist List serves as a vital tool in countering the financing of terrorism and extremism in the Russian Federation. An analysis of the statistical data presented in Figure 1 provides insight into its effectiveness.

Also, when reviewing the structure and composition of the Terrorist and Extremist List by territory, a notable trend emerges in the quantitative changes of listed entities in the Central Federal District (CFD).

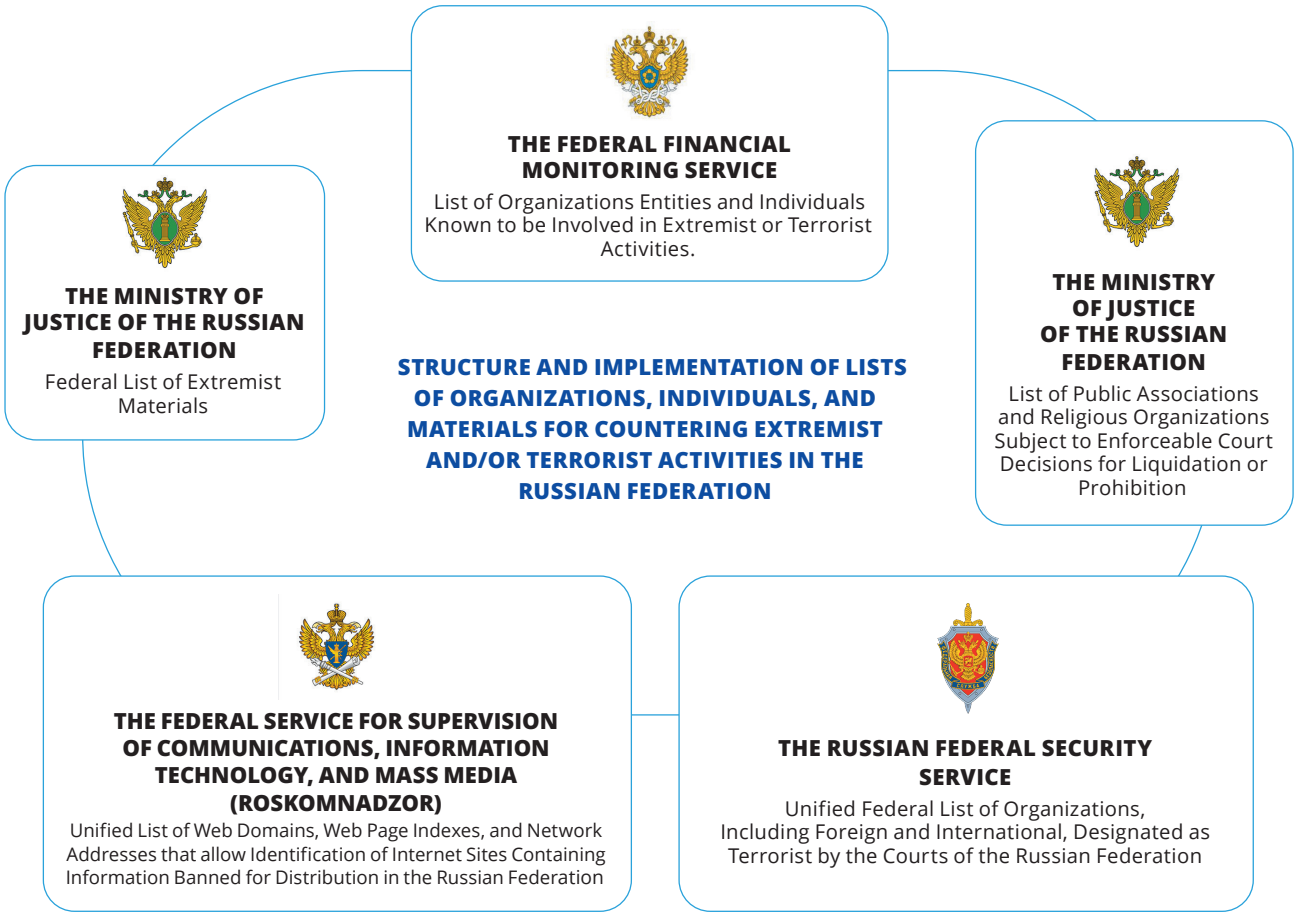
The number of entities listed in the CFD fluctuates in alignment with the overall national trend, reflecting a consistent pattern.

Over the reporting period, the CFD accounted for an average of 17% of the total entities on the list, with a range of 12% to 28%.

This fact indicates that the trends in terrorist and extremist risks and threats in the CFD are similar to those across the country.

The CFD's mirroring in these trends can be attributed to the concentration of financial and human resources in the Moscow

▸ **Figure 2.**



region, as well as incorporation of certain regions bordering the combat contact zone.

In concluding the review of terrorist and extremist lists as one of the effective counteraction tools, it is essential to differentiate them by type, measures, and vectors of control, which are tailored to address distinct aspects of terrorist and extremist activities.

By sharing these lists, law enforcement agencies, executive bodies, and other government institutions are equipped with critical tools to maintain security, uphold the rule of law, and protect national interests. However, it is important to remember that each mechanism plays a unique role in ensuring security and social stability.

ANTI-MONEY LAUNDERING NEWS

MOSCOW: WORKING MEETING HELD BETWEEN FFMS AND DELEGATION OF EXECUTIVE COMMITTEE OF SCO RATS

German Neglyad, State Secretary and Deputy Director of the FFMS, emphasized the high level of cooperation between the Russian Financial Intelligence Unit and the SCO RATS in countering the financing of terrorism and extremism. Ularbek Sharsheev, SCO RATS Director acknowledged Russia's contributions into the work of the structure and emphasized the importance of coordinated common efforts among the SCO member states in addressing emerging challenges and threats.

VIENNA: MEETING OF GROUP OF EXPERTS ON COUNTERING PROLIFERATION FINANCING (CPF)

Organized under the UNODC's Global Program against Money Laundering, Proceeds of Crime, and the Financing of Terrorism (GPML), this meeting brought together experts to discuss inter-agency collaboration, new typologies, national risk assessments, international CPF mechanisms, and other topics.

BANGKOK: ASIA-PACIFIC REGIONAL PREPARATORY MEETING FOR 15TH UN CONGRESS ON CRIME PREVENTION AND CRIMINAL JUSTICE

The meeting was hosted by the UN Economic and Social Commission for Asia and the Pacific (ESCAP) and attended by representatives of relevant ministries and agencies, including the Federal Financial Monitoring Service, from more than 20 countries. FFMS officers presented latest regulatory updates to the Russian AML/CFT system, shared best practices in anti-money laundering, as well as

their experience in identifying new means and methods of terrorist financing. The meeting emphasized the importance of collaborative efforts to identify global terrorist financing networks and combat this international threat.

MINSK: SEMINAR FOR MEMBER STATES OF EURASIAN GROUP ON COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM (EAG) ON FINANCIAL ACTION TASK FORCE (FATF) STANDARDS

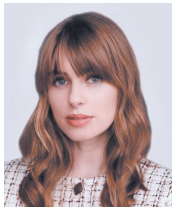
Organized by the EAG Secretariat and the Financial Monitoring Department of the State Control Committee of the Republic of Belarus, the seminar aimed to deepen understanding of the FATF standards and their implementation across EAG member states, while also training a pool of expert assessors.

EDITORIAL BOARD

Chairman:
Yu. Chikhanchin

Deputy Chairman:
V. Ovchinnikov

Deputy Chairman:
G. Neglyad



Editor-in-chief:
I. Ryazanova

BOARD MEMBERS

G. Bobrysheva

E. Gileta

I. Kornev

O. Krylov

A. Lisitsyn

A. Petrenko

S. Teterukov

I. Uvarov

M. Shemyakina

FFMS and ITMCFM on Telegram and VKontakte

Publishing House
International Training and Methodology Center for Financial Monitoring
Autonomous non-profit organization
#31 Staromonetny Lane, Bldg. 1, Moscow, 119017
E-mail: info@mumcfm.ru

ITMCFM
2025