UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
Programme Office in Doha

Parliamentary Engagement
in Preventing and Countering Terrorism

ICRC

مجلس الشورى
The Shura Council
State of Qatar • دولة قطر

OUTCOME DOCUMENT

CONFERENCE

“Legislative Regulation of Measures to Counter the Use of Artificial Intelligence and Other New Technologies for Terrorist Activities”

Saint Petersburg, Russian Federation

17 April 2025

КОНФЕРЕНЦИЯ
Законодательное регулирование противодействия использованию искусственного интеллекта и новых технологий в террористических целях
CONFERENCE
Legislative Regulation of Measures to Counter the Use of Artificial Intelligence and Other New Technologies for Terrorist Activities
Санкт-Петербург, Российская Федерация
Saint Petersburg, Russian Federation
17 апреля 2025 года
17 April 2025

This document does not constitute official conclusions, nor is it an exhaustive record of all issues raised during the Conference. It is intended as a collection of relevant points, key takeaways, and recommendations for potential future reference. While the United Nations Office of Counter-Terrorism (UNOCT) strives to ensure the accuracy and relevance of the information presented, it makes no claims or warranties, express or implied, regarding the completeness, accuracy, or reliability of the content. The views and recommendations included are solely offered for reference and should not be interpreted as conclusive or comprehensive.

1. EXECUTIVE SUMMARY

The Conference titled *“Legislative Regulation of Measures to Counter the Use of Artificial Intelligence and Other New Technologies for Terrorist Activities”* took place on 17 April 2025 in Saint Petersburg, Russian Federation, alongside the Fifty-Eighth Plenary Session of the Inter-Parliamentary Assembly of Member Nations of the Commonwealth of Independent States (IPA CIS). Convened by the United Nations Office of Counter-Terrorism (UNOCT) Programme Office on Parliamentary Engagement in Preventing and Countering Terrorism with the support of the Shura Council of the State of Qatar, and in collaboration with the Interparliamentary Assembly of Member Nations of the Commonwealth of Independent States the (IPA CIS) and the International Committee of the Red Cross (ICRC).

The Conference gathered over 120 participants representing national parliaments, regional and international parliamentary assemblies, international and regional organizations, the private [technology] sector, academia, and civil society. Among the parliamentary assemblies represented were the African Parliamentary Union (APU), Arab Parliament, Asian Parliamentary Assembly (APA), Interparliamentary Assembly of Member Nations of the Commonwealth of Independent States the (IPA CIS), Parliamentary Assembly of the Black Sea Economic Cooperation (PABSEC), Parliamentary Assembly of the Mediterranean (PAM), Parliamentary Assembly of the Organization for Security and Co-operation in Europe (OSCE PA), Latin American and Caribbean Parliament (PARLATINO), Parliamentary Union of the OIC Member States (PUIC), and the Parliamentary Assembly of Turkic States (TURKPA).

Discussions benefited from the expertise of representatives from UNOCT’s Cybersecurity and New Technologies Unit, the UN Security Council’s Counter-Terrorism Committee Executive Directorate (CTED), the ICRC, and regional security organizations including the Regional Anti-Terrorism Structure of the Shanghai Cooperation Organization (SCO RATS), the SCO Secretariat, and Commonwealth of Independent States Anti-Terrorism Center (CIS ATC). Contributions were also made by private sector actors and academic institutions, including the Research Center of the Federal Security Service (FSB) of Russia, LLC “NOTBOT” of the Republic of Belarus, the RUSSOFT Association, PIX Robotics, and ITMO University (St. Petersburg National Research University of Information Technologies, Mechanics and Optics).

The Conference was structured around three thematic segments: i) Parliamentary perspectives and legislative efforts; ii) International standards and legal frameworks; iii) and the Contribution of the private sector, academia, and research. Discussions focused on the implications of artificial intelligence and emerging technologies for both terrorism and counter-terrorism operations. Particular attention was given to oversight and accountability challenges, humanitarian risks, and the existing legal and ethical gaps surrounding these technologies.

Participants emphasized the need for rights-based regulatory approaches that uphold international humanitarian law (IHL) and international human rights law (IHRL), while addressing legitimate security concerns. The Conference facilitated a dialogue on the complexities of AI governance, encouraged the identification of good practices, and laid the groundwork for the development of model legislation. It also reinforced inter-institutional cooperation among UNOCT, IPA CIS, ICRC, and national parliaments and led to the articulation of guiding principles for future legislative initiatives aimed at ensuring the ethical, lawful, and secure use of AI in counter-terrorism efforts.

2. BACKGROUND

In recent years, artificial intelligence has emerged as one of the most transformative technological forces of our time. Its capacity to revolutionize science, public services, and industry is accompanied by mounting concerns over its unintended consequences for societies and governments worldwide. In addition to its economic and social impacts—such as job displacement and increased societal vulnerabilities—AI presents significant challenges in the security domain. Its rapid development and increasingly accessible capabilities have raised the alarm over its potential misuse by terrorist actors, who may exploit AI systems to plan, facilitate, or execute attacks. This threat underscores the urgent need for well-defined, rights-based legislative responses at both the national and international levels.

The urgency of addressing AI in the context of terrorism and counter-terrorism was notably highlighted during the Fourth Parliamentary Policy Dialogue held in Rome on 5 December 2024. Organized by the UNOCT Programme Office on Parliamentary Engagement in collaboration with the OSCE Parliamentary Assembly, the Dialogue revealed widespread concerns among parliamentarians about the lack of adequate legislative frameworks to govern the use of AI and emerging technologies in counter-terrorism while preventing their exploitation by terrorist groups. Participants called for enhanced cooperation and technical support to close these regulatory gaps and ensure alignment with international legal standards.

In this context, the UNOCT Programme Office on Parliamentary Engagement—serving as a dedicated hub within the United Nations system supporting parliamentary action in counter-terrorism and prevention of violent extremism—has been actively engaged in identifying priority areas requiring technical assistance. As the Secretariat of the Coordination Mechanism for Parliamentary Assemblies on Counter-Terrorism, the Programme Office regularly consults its partnering assemblies to assess evolving needs. A recent survey among the Mechanism's participants confirmed that the governance of new technologies, particularly artificial intelligence, is a top concern demanding coordinated response.

Against this backdrop, there was a clear need to convene a dedicated, multilateral platform where legislators and experts could address the emerging risks associated with the use of artificial intelligence in terrorism and counter-terrorism. Such a platform would enable the exchange of legislative experiences, enhance mutual understanding of the challenges posed by rapidly evolving technologies, and support the formulation of coherent and rights-respecting legal responses. The Conference was conceived to respond to this need by fostering dialogue, promoting legal harmonization, and exploring avenues for international cooperation on this pressing and complex issue.

3. KEY DISCUSSIONS BY SEGMENT

3.1. Parliamentary Perspectives and Efforts

The main part of the Conference was dedicated to interventions by international parliamentary assemblies participating in the Coordination Mechanism for Parliamentary Assemblies on Counter-Terrorism. These interventions highlighted regional parliamentary perspectives and efforts in preventing and countering terrorism, with a particular focus on legislative responses to AI and emerging technologies. Speakers shared national and regional experiences while reflecting on the evolving role of national parliaments and parliamentary assemblies in promoting rights-based, security-conscious policy frameworks.

Several presentations offered concrete examples of how parliamentary assemblies are actively responding to the security challenges posed by emerging technologies. Among the notable contributions were those from PAM, OSCE PA, and IPA CIS, each highlighting distinct legislative approaches and practical initiatives.

The PAM underlined the critical role of parliaments in addressing the misuse of AI and emerging technologies by terrorist and criminal actors. PAM highlighted its efforts and several of its Member States—Algeria, Saudi Arabia, and the UAE—in advancing legislation and ethical frameworks aligned with international law and the protection of fundamental rights. Among PAM's flagship initiatives is the work of the PAM Centre for Global Studies (CGS), which published a joint report with the UN Security Council Counter-Terrorism Executive Directorate (CTED) on the Malicious Use of AI and Emerging Technologies by Terrorist and Criminal Groups. This report led to the establishment of the *Global Permanent Parliamentary Observatory on the Misuse of AI and ICT*, based in San Marino, which issues a daily *Digest* tracking global developments in the field.

PAM's collaboration with CTED continues through a peer-reviewed research project titled *Spyware Misuse: Legislative, Governance, and Judicial Considerations, Historical Evolution, and Technical Insights*, which is expected to be presented at the 80th UN General Assembly. Additionally, PAM supports the UN-led consultative process to establish an *Independent International Scientific Panel on AI*, aimed at strengthening global governance and enhancing understanding of AI-related risks. PAM also reported on its recent work on the Valletta Principles on National and Regional Counter-Terrorism Strategies, presented during an online seminar on 9 May, following a UN-sponsored meeting in Malta.

The OSCE Parliamentary Assembly's Resolution on Artificial Intelligence and the Fight Against Terrorism, adopted in Bucharest in June 2024, was also presented as a key international reference point for addressing the dual-use nature of AI. The OSCE PA emphasized the Resolution's balanced approach, which promotes the use of AI in counter-terrorism while safeguarding human rights, fundamental freedoms, and the rule of law. The Resolution calls for strengthened legal frameworks, robust ethical standards, and effective oversight mechanisms. It further advocates for public-private partnerships, mandatory labeling of AI-generated content, and media literacy initiatives to foster societal resilience.

The OSCE PA continued efforts to operationalize the Resolution's provisions were highlighted at the *Fourth Parliamentary Policy Dialogue*, held in Rome in December 2024. OSCE PA also referenced its Ad Hoc Committee on Countering Terrorism in key global platforms, including the Internet Governance Forum in Riyadh, as well as official visits to Türkiye, which facilitated the exchange of best practices and reinforced multilateral cooperation. These initiatives underscored the OSCE PA's commitment to a proactive and rights-based approach in countering AI-related security threats.

In their interventions, representatives of the IPA CIS highlighted their ongoing legislative contributions to AI governance and counter-terrorism. They drew particular attention to the adoption, in April 2025, of the Model Law On Artificial Intelligence Technologies, developed in collaboration with the United Institute of Informatics Problems of the National Academy of Sciences of Belarus. This model law provides a comprehensive legal and ethical framework for the secure development and application of AI across CIS countries. It encourages the use of shared terminology, state-supported AI integration across key sectors, and the incorporation of technological impact assessments into legislative processes. The initiative aligns with the agendas of the United Nations General Assembly and the International Telecommunication Union.

In parallel, IPA CIS is finalizing the *Model Law On Countering the Use of Autonomous and Robotic Systems for Terrorist and Extremist Purposes*, which responds to the growing risk of AI-enabled technologies being exploited for malicious purposes. Representatives emphasized the need for clear legal mechanisms to hold both system developers and end-users accountable, particularly as autonomous technologies become increasingly accessible. These efforts reflect IPA CIS's broader commitment to advancing good international and regional parliamentary practices in regulating AI. Parliamentary assemblies, they noted, are well placed to promote the application of this expertise in other regions, facilitating inter-parliamentary cooperation, the exchange of best practices, and the harmonization of legal responses to AI-related security challenges.

The Parliamentary Assembly of the Black Sea Economic Cooperation (PABSEC) highlighted the increasing international relevance of artificial intelligence and new technologies in the context of counter-terrorism. The Assembly emphasized that the growing complexity of security threats requires the adoption of comprehensive legislation that addresses the dual-use nature of these technologies. PABSEC stressed the importance of ensuring that legal frameworks are forward-looking and capable of balancing technological innovation with the protection of human rights and fundamental freedoms.

In its intervention, PABSEC noted its intention to further explore the potential of AI through upcoming discussions within its committees, particularly in relation to its application for sustainable socio-economic development. It acknowledged that the legislative response to AI should not only focus on risk mitigation but also recognize the opportunities AI presents when applied responsibly. The Assembly reaffirmed the necessity of regional cooperation in the development of harmonized legal standards that reflect both security needs and democratic values.

The Parliamentary Assembly of Turkic States (TURKPA) underscored the urgent need for coherent legislative responses to the evolving threat posed by artificial intelligence and other new technologies when misused by terrorist actors. TURKPA warned that if left unregulated, such technologies could amplify terrorist organizations' capabilities in areas such as propaganda dissemination, encrypted communications, and cyberattacks. It was emphasized that effective legal frameworks must be developed to ensure that AI systems remain transparent, ethically governed, and fully compliant with human rights standards.

TURKPA called for the establishment of common international norms that promote cross-border cooperation, information-sharing, and standard-setting to address the transnational nature of AI-related security threats. The Assembly advocated for closer collaboration between technology companies and state institutions to enhance early warning mechanisms, cybersecurity infrastructure, and public awareness. It emphasized that public education on the risks and benefits of AI, combined with clear regulatory mandates, is vital to preventing the misuse of emerging technologies and strengthening societal resilience. TURKPA concluded that a unified legal framework—developed at both national and international levels—is essential to safeguard public security and uphold the rule of law in the digital age.

3.2. International Organizations, Standards, and Legal Frameworks

Following the parliamentary perspectives, delegates from international organisations shared their views on the relevant international standards, legal frameworks and measures pertaining to the necessary legislative and regulatory measures to counter the use of AI and Other emerging technologies for terrorist activities.

The International Committee of the Red Cross (ICRC) emphasized that the growing use of AI in counter-terrorism presents urgent and complex humanitarian concerns. As a neutral and independent organization working in armed conflict and other situations of violence, the ICRC has observed first-hand how emerging technologies—when deployed without appropriate safeguards—can heighten risks to civilian populations, hinder humanitarian access, and influence life-and-death decisions. It warned that AI's use in high-risk contexts, such as autonomous weapons systems and decision-support tools, can raise serious legal, ethical, and operational challenges.

The ICRC stressed that AI is not inherently good or bad, but a set of tools that must be governed responsibly. While the ICRC itself uses AI and digital technologies to improve operations in areas like logistics and healthcare, it underscored the need for strong internal governance, technical expertise, and a precautionary approach to risk management. It also raised concerns about the potential misuse of AI by malicious cyber actors, including those targeting humanitarian organizations.

From a legal and ethical standpoint, the ICRC called for the integration of humanitarian safeguards into national and international legislative and regulatory frameworks. It argued that responses to AI in counter-terrorism must go beyond security imperatives and place human dignity, accountability, and respect for the International humanitarian law (IHL) at the center. Human judgment, the ICRC noted, must remain essential in all AI-supported decision-making processes. Machines cannot replace the legal responsibilities borne by human actors, particularly in armed conflict, where IHL requires clear, accountable decision-making based on legal determinations.

The ICRC expressed particular concern about AI systems' potential to perpetuate biases, generate errors, and obscure accountability due to increasing complexity and lack of transparency. It highlighted the risks of automation bias, where overreliance on machine outputs can lead decision-makers to become passive executors rather than responsible agents. To mitigate these risks, it called for meaningful human control, robust oversight mechanisms, and the development of new, binding international rules on autonomous weapons systems—specifically those that are unpredictable or designed to target humans directly.

Beyond weapon systems, the ICRC warned that counter-terrorism measures using AI—if not designed in accordance with international law—could have unintended negative effects on humanitarian action and populations in need of protection. It welcomed Security Council Resolutions 2462 and 2482, which acknowledge these risks and call on States to comply with IHL. The ICRC strongly supported the inclusion of humanitarian carve-outs in AI-related counter-terrorism policies to ensure that such measures do not adversely affect impartial humanitarian action.

The ICRC concluded by urging States and parliaments to ensure that legislative and policy frameworks on the use of AI in counter-terrorism reflect obligations under IHL, include mechanisms for accountability and transparency, and are developed through inclusive, multi-stakeholder dialogue. Parliaments, in particular, were called upon to play a leading role in ensuring that technological progress does not come at the expense of fundamental rights and protections. By placing people—especially those most at risk—at the center of policy decisions, AI can serve as a tool not only for security, but also for humanity.

The UNOCT Programme Office on Parliamentary Engagement in Preventing and Countering Terrorism emphasized that while artificial intelligence and other emerging technologies offer new opportunities to enhance counter-terrorism responses, their misuse by terrorist actors raises serious legal, ethical, and security concerns. Addressing these challenges requires timely, coordinated, and forward-looking legislative action at both national and international levels.

Building on the outcomes of the *Fourth Parliamentary Policy Dialogue* held in Rome in December 2024, the Programme Office underscored that the Conference serves as a critical platform to examine the implications of AI and other new technologies in the context of terrorism. It aims to identify gaps in existing legal frameworks, share good practices, and work toward the development of a model legal framework that balances technological innovation, security imperatives, and the protection of human rights.

The Programme Office also highlighted its broader efforts to support inclusive and rights-based legislative approaches, including its role as the Secretariat of the Coordination Mechanism for Parliamentary Assemblies on Counter-Terrorism. Through this role, it facilitates sustained inter-parliamentary dialogue, promotes legal coherence, and encourages the sharing of expertise and good practices among parliamentary assemblies worldwide. The Programme Office reaffirmed its commitment to advancing practical, cooperative solutions rooted in international law and aligned with core human rights principles.

The UNOCT Programme Office on Parliamentary Engagement underscored that the rapid advancement of artificial intelligence and other emerging technologies had introduced both promising opportunities and significant challenges for global counter-terrorism efforts. Recognizing the complex legal, ethical, and humanitarian concerns these technologies raise—particularly regarding their potential misuse by terrorist actors and the associated risks—the Programme Office has been actively working to raise awareness among national parliaments and parliamentary assemblies worldwide. Its efforts focus on highlighting the wide spectrum of issues, challenges, and opportunities that AI and new technologies present, while promoting practical, rights-based legislative and policy solutions that align with international standards and good practices.

The Cybersecurity & New Technologies Unit of the United Nations Office of Counter-Terrorism / United Nations Counter-Terrorism Centre (UNOCT/UNCCT) presented an in-depth overview of the risks and regulatory challenges associated with the use of AI for terrorist purposes. It was noted that AI encompasses a wide array of systems capable of performing tasks typically requiring human intelligence, and while such technologies offer significant promise, they also present serious risks when exploited by terrorist actors. Referring to the New Agenda for Peace released by the UN Secretary-General in July 2023, the presentation emphasized that the increasing power and accessibility of generative AI—such as deepfakes—pose growing threats to political stability, public trust, and civilian safety.

Key findings from the UNOCT-UNCCT and UNICRI joint Report on the Malicious Use of Artificial Intelligence for Terrorist Purposes were highlighted, identifying a spectrum of AI-driven threats, including enhanced cyberattacks, autonomous weapons, disinformation campaigns, and bioengineered weapons. These challenges underscore the urgent need for regulatory frameworks that integrate humanitarian and human rights safeguards, in line with relevant UN resolutions such as Security Council Resolutions 2178, 2370, and 2396, the Madrid Guiding Principles, and the Delhi Declaration.

To support Member States in addressing these threats, the presentation outlined several UNOCT initiatives. These include the Cybersecurity and New Technologies programme, which helps build resilience to cyberattacks on critical infrastructure, and the CT TECH and CT TECH+ initiatives, developed in partnership with INTERPOL and funded by the European Union, which enhance law enforcement and judicial capacities in a human rights-compliant and gender-responsive manner. The Unit also provides capacity-building in areas such as unmanned aerial systems, open-source intelligence, dark web investigations, and digital forensics.

The presentation concluded with a call for coordinated, rights-based approaches to AI governance, stressing that AI is not only a technological tool but also a matter of ethical responsibility and judgment. It emphasized that legislative and regulatory measures must evolve in parallel with technological advancements to effectively prevent the misuse of AI by terrorist actors. Such measures should clearly define the boundaries of acceptable use, ensure oversight and accountability, and be grounded in international law, including international humanitarian and human rights law. Effective responses will require close cooperation between governments, private sector actors, and civil society to ensure that AI serves peace and security rather than exacerbating threats.

The Counter-Terrorism Committee Executive Directorate (CTED) underscored the growing importance of developing responsible and effective legislative and regulatory frameworks to address the use of artificial intelligence (AI) for terrorist purposes. As part of its Security Council mandate, CTED conducts technical assessments of Member States' implementation of counter-terrorism obligations and facilitates technical assistance. Through this work, CTED has identified several emerging practices related to AI, including safety-by-design approaches, ethical programming, impact assessments, and digital literacy initiatives that strengthen societal resilience to AI-driven terrorist content and online fundraising.

CTED emphasized that as parliamentarians develop legislative responses to AI-related terrorist threats, it is crucial not to reinvent the wheel. Numerous frameworks, initiatives, and instruments—such as the United Nations Global Digital Compact, ASEAN's Guide on AI Governance and Ethics, and resolutions by the PAM—already provide strong foundations. Rather than creating new laws from scratch, CTED recommended reviewing and amending existing national legislation to account for the use of digital and AI technologies in terrorist contexts. Laws that currently cover traditional propaganda or recruitment, for instance, could be expanded to address digital content dissemination.

Importantly, CTED advised that legislation should regulate not only how non-State actors use AI for terrorism but also how States deploy AI in counter-terrorism, including in surveillance, digital evidence collection, and investigative practices. These uses must be grounded in international law, particularly international human rights and humanitarian law, to prevent overreach and protect privacy and due process. The development of human rights impact assessments, including gender-sensitive evaluations, was highlighted as essential to anticipate and mitigate potential unintended consequences.

CTED further advocated for a whole-of-society approach to legislation, encouraging inclusive stakeholder engagement, public consultations, and public-private partnerships to ensure that AI-focused regulations are comprehensive, technologically informed, and adaptable to future developments. Special attention was drawn to the need for cross-border legal harmonization to address the jurisdictional challenges posed by the borderless nature of digital terrorism. CTED concluded by reaffirming the critical role of parliamentarians in building effective, inclusive, and rights-based counter-terrorism frameworks, and expressed its readiness to support Member States in crafting solutions that are both impactful and sustainable.

3.2. Security and Law Enforcement Sector

Participation of representatives from international and regional security institutions and organisations enriched the discussion and deepened understanding of the multifaceted issues related to the use of artificial intelligence (AI) and new technologies in counter-terrorism. Three interventions from the Commonwealth of Independent States (CIS) community—the CIS Anti-Terrorism Center (CIS ATC), its Scientific and Advisory Council, and the broader CIS ATC leadership—offered a comprehensive regional perspective on legal, operational, and strategic dimensions.

The CIS ATC emphasized the growing threat posed by the misuse of AI and new technologies for terrorist purposes and called for strengthened regional legal responses. Against the backdrop of geopolitical instability and the weakening of international institutions, the CIS ATC stressed the importance of advancing Eurasian legal integration and collaborative legislative action among CIS member states. The Center's contribution to the development and refinement of model laws under the IPA CIS has been instrumental, particularly in the areas of national security, cybercrime, border security, and counter-terrorism.

A major point of focus was the draft CIS Model Law *On Countering the Use of Artificial Intelligence and Robotics for Terrorist and Extremist Purposes*, developed within the framework of the 2023–2025 Cooperation Programme of CIS Member States in Combating Terrorism and Other Violent Manifestations of Extremism. This initiative aims to address the absence of precise legal definitions and harmonized standards for autonomous systems. It draws upon a range of regional and international sources, including the CIS Heads of State Statement on Civilian AI, the Kazan Declaration, CSTO Parliamentary Assembly recommendations, and the Union State Security Concept. The draft is designed to align emerging technologies with security priorities while ensuring legal coherence with the CIS Model Law *On Artificial Intelligence Technologies*.

The CIS ATC also contributed to the draft Model Law *On Public Security*, expected to be adopted by the IPA CIS soon. This would allow for the preparation of detailed commentaries to support legislative implementation. Looking ahead, the CIS ATC is exploring further model legal acts covering national security, chemical terrorism, operational investigative measures, and the integration of international humanitarian law into regional responses involving autonomous systems. The Center highlighted its productive cooperation with the Shanghai Cooperation Organisation's Regional Anti-Terrorist Structure (SCO RATS) and announced plans to co-host a follow-up event in Dushanbe, Tajikistan, later in the year.

In conclusion, the CIS ATC advocated for institutionalizing annual joint counter-terrorism conferences and proposed including the discussed legislative initiatives in the next IPA CIS Council decision. It reaffirmed its commitment to advancing a harmonized legal framework through coordinated, cooperative engagement.

Complementing this intervention, the Scientific and Advisory Council under the CIS ATC stressed the urgency of a robust scientific and legal response to the integration of AI into terrorist activities. Recent regional statistics underscored a significant concentration of terrorism-related crimes in CIS countries, demanding regulatory attention to AI, unmanned systems, robotics, and digital financing.

The Council highlighted the risks inherent in AI technologies, including their dual-use nature, opacity, and accelerating autonomy. These risks extend beyond security threats, encompassing broader societal challenges such as disinformation, social isolation, loss of autonomy, and negative impacts on mental health and child development. The proliferation of deepfakes, AI-driven propaganda, and systems like *Oculus* that detect illicit content illustrate the dual-edged nature of AI applications in the information space.

The Council called for harmonized legal norms across technical, ethical, and legal domains. It welcomed the 2024 Statement on Cooperation in Civilian AI by CIS Heads of State, which advocated for state oversight, robust digital infrastructure, and a central coordinating role for the UN in global AI governance. The Council further emphasized the need to define “red lines” for AI use in national security contexts, alongside mechanisms for testing, verification, and accountability.

The IPA CIS Recommendations on the Legal Regulation of AI were acknowledged as key instruments, particularly their emphasis on ethical safeguards against manipulation and discrimination. Recent legislative efforts, such as amendments introducing AI as an aggravating factor in criminal law, were welcomed. The Council also urged development of criminological forecasting, protections against biometric misuse, and enhanced identification technologies for border and migration control.

In its closing message, the Council called for a comprehensive legal and ethical regime to prevent the exploitation of AI for terrorist purposes. It advocated for a balanced approach that combines general restrictions with targeted norms, reinforced by public awareness, digital literacy, fact-checking, and safeguards for digital sovereignty.

The broader CIS ATC leadership welcomed the Conference as a timely initiative addressing the rapidly evolving threat landscape. It acknowledged the 25-year legacy of joint CIS counter-terrorism efforts and noted that instability in regions such as Afghanistan and the Middle East continues to fuel radical ideologies targeting youth and vulnerable communities.

The Center noted that terrorist groups increasingly exploit AI and digital technologies for propaganda, recruitment, encrypted communications, attack coordination, and funding. The production and dissemination of convincing AI-generated fake content was identified as an urgent threat, requiring prompt regulatory attention. These themes have already been addressed in IPA CIS deliberations on public security and deradicalization.

Through expert presentations, the CIS ATC reaffirmed its intention to align regional legislative development with international standards. It expressed interest in enhanced engagement with the UNOCT, particularly through its interparliamentary initiatives such as the upcoming Counter-Terrorism Forum in Dushanbe.

Looking to the future, the CIS ATC emphasized its role in shaping the next Long-Term Plan for CIS Model Legislative Work, reaffirming its commitment to strengthening collective responses through cooperation with the IPA CIS and international partners. The Center concluded by underscoring the importance of international legal collaboration to ensure security, legal consistency, and resilience in the face of AI-enabled terrorist threats.

3.3. Private Sector, Research, and Academia

The participation of representatives from the private sector, academic institutions, and research organizations brought valuable perspectives to the conference. Their contributions underscored the essential role that technological innovation, interdisciplinary research, and cross-sectoral collaboration play in confronting the growing risks associated with the misuse of AI and new technologies for terrorist purposes.

Discussions emphasized that the rapid development and deployment of AI often outpace existing legal and regulatory frameworks, highlighting both the promise of technological advancement and the challenges it poses. Participants stressed the necessity of fostering robust public-private partnerships to ensure that AI is developed and applied in ways that are secure, ethical, and aligned with human rights principles.

Research institutions emphasized the importance of comprehensive risk assessments, the integration of security-by-design principles, and the implementation of technical safeguards to prevent the misuse of AI. They highlighted the need for greater algorithmic transparency, improved data governance, and the establishment of accountability mechanisms to build trust and resilience in AI systems.

Academia further emphasized the importance of interdisciplinary education and training to equip future experts with the competencies required to navigate the societal, legal, and security implications of emerging technologies. Developing curricula that integrate technical expertise with ethical awareness was identified as a critical step toward responsible innovation.

The private sector emphasized that, while it plays a leading role in the development of AI, it also bears a responsibility to anticipate and mitigate potential threats stemming from its misuse. Industry representatives advocated for enhanced cooperation and information sharing with policymakers, regulators, and civil society to ensure that AI applications contribute to collective security.

Speakers collectively acknowledged the pivotal role of adequate legislation and regulation in supporting a secure and responsible innovation environment. Effective legal frameworks can offer the clarity, incentives, and protections necessary for the private sector, researchers, and scientists to operate responsibly while mitigating risks. Policymakers were encouraged to maintain close engagement with technical and industry experts to ensure that legislation remains adaptive, effective, and aligned with international standards.

In conclusion, the session reaffirmed that safeguarding against the terrorist exploitation of AI and new technologies requires a whole-of-society approach. The contributions of the private sector, academia, and research communities are indispensable to shaping resilient and future-ready strategies. Their active engagement is crucial in ensuring that technological progress is guided by ethical foresight, inclusivity, and a steadfast commitment to human security.

4. KEY FINDINGS, RECOMMENDATIONS AND FOLLOW-UP ACTIONS

The Conference underscored the growing consensus among parliamentarians, international organizations, humanitarian actors, and technical experts on the urgency of addressing the dual-use nature of artificial intelligence and emerging technologies in the context of terrorism and counter-terrorism. Participants collectively recognized that while AI holds significant potential to enhance security operations, its misuse by terrorist actors introduces unprecedented legal, ethical, and operational challenges that demand timely, inclusive, and coordinated responses.

One of the most prominent findings of the Conference was the identification of significant gaps in existing national and international legal frameworks concerning the use and regulation of AI in counter-terrorism. Participants emphasized that the rapid pace of technological advancement has outstripped current legislation, creating regulatory blind spots and inconsistent standards across jurisdictions. To address this, the development of a model legislative framework grounded in international humanitarian law and international human rights law was highlighted as a critical need. Such a framework should incorporate principles of transparency, accountability, ethical safeguards, and effective oversight mechanisms.

The Conference also highlighted the importance of a human-centred approach to AI governance. Across all thematic segments, participants stressed that human judgment and accountability must remain central in the design, deployment, and use of AI technologies, particularly in high-risk security and humanitarian contexts. In addition, the need for meaningful multi-stakeholder engagement, including the private sector, academia, and civil society, was emphasized as essential to crafting holistic and future-proof solutions.

Based on these findings, the following key recommendations emerged:

- Support the development of a rights-based, internationally aligned model legal framework to regulate the use of AI and emerging technologies in counter-terrorism efforts;
- Strengthen the capacity of national parliaments to legislate and provide oversight on AI and emerging technologies, including through technical assistance, expert consultations, and peer exchange;
- Foster inter-parliamentary dialogue to promote harmonized legislative responses and the sharing of good practices;
- Enhance cooperation between national parliaments, governments, the private sector, and research communities to ensure that innovation is balanced with risk mitigation;
- Prioritize humanitarian carve-outs and safeguards in counter-terrorism legislation to protect impartial humanitarian action and at-risk populations;
- Advance public awareness, digital literacy, and algorithmic transparency to reduce vulnerabilities and build societal resilience against AI-driven threats.

As a concrete follow-up, the Conference resulted in a preliminary list of joint activities to be explored by the UNOCT Programme Office on Parliamentary Engagement, IPA CIS, and the ICRC, in close collaboration with interested national parliaments. These activities include the development of model legislative provisions, capacity-building workshops, and thematic briefings designed to support national-level implementation of effective, ethical, and rights-based AI regulation in counter-terrorism.

5. CONCLUSIONS

The Conference served as a timely and action-oriented platform for dialogue, collaboration, and strategic thinking on one of the most complex and fast-evolving challenges in contemporary counter-terrorism: the regulation of artificial intelligence and other emerging technologies. It reaffirmed the collective recognition that ensuring security in the age of AI requires not only technological preparedness but also a strong commitment to international law, ethical governance, and institutional cooperation.

The discussions held across the parliamentary, institutional, and technical segments revealed a shared determination to move from awareness to action. Delegates acknowledged the limitations of existing legal frameworks and called for targeted, coordinated efforts to fill these gaps while upholding the principles of legality, accountability, and proportionality. It was widely agreed that parliamentary institutions have a unique and indispensable role to play in this process, given their legislative mandates, oversight functions, and capacity to bridge the gap between global norms and national implementation.

The Conference concluded with a call to sustain and expand the partnerships established through this event. Participants expressed strong interest in continuing the exchange of knowledge and best practices, advancing legislative solutions, and fostering a unified approach to countering the misuse of AI for terrorist purposes. Through collaborative efforts, informed policymaking, and inclusive dialogue, stakeholders committed to ensuring that the use of new technologies in counter-terrorism remains consistent with the protection of human rights, the rule of law, and international peace and security.

6. COMMUNICATIONS

Press releases

https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20250417_parliamentai_press_release_final.pdf

https://iacis.ru/News/Partners/International_Conference_in_St_Petersburg_Focuses_on_Preventing_Use_of_AI_for_Terrorist_Purposes

https://www.oscepa.org/en/news-a-media/news-from-copenhagen/2025/5210-news-from-copenhagen-1007/file

https://pam.int/pam-contributes-to-the-un-led-global-dialogue-on-legal-frameworks-to-address-the-misuse-of-ai-by-terrorist-groups/

https://www.pabsec.org/news-detail/participation-of-mr-asaf-hajiyev-pabsec-secretary-general-in-the-unoct-international-conference-st-petersburg-17-april-2025/720

https://turkpa.org/tr/news/1804-turkpa-participated-in-the-international-conference-on-counter-terrorism-in-st-petersburg

https://www.eng.cisatc.org/1289/136/9138/9620

Tweets

https://x.com/UN_OCT/status/1913069673156870350?