OUTCOME DOCUMENT

FOURTH PARLIAMENTARY POLICY DIALOGUE ON COUNTERING THE USE OF ARTIFICIAL INTELLIGENCE AND NEW TECHNOLOGIES FOR TERRORIST PURPOSES

Rome, Italy
5 December 2024

EXECUTIVE SUMMARY

The [United Nations Office of Counter-Terrorism](#) (UNOCT) [Programme Office on Parliamentary Engagement in Preventing and Countering Terrorism](#) and the [UNOCT Cybersecurity & New Technologies Unit](#), with the support of [the Shura Council of the State of Qatar](#), and in collaboration with [the Parliamentary Assembly of the Organization for Security and Cooperation in Europe (OSCE PA)](#), organized the Fourth Parliamentary Policy Dialogue on "Countering the Use of AI and New Technologies for Terrorist Purposes." Hosted by the Italian Parliament in Rome on 5 December 2024, the event convened over 70 in-person and 10 online participants, including representatives from parliamentary assemblies, national parliaments across Africa, Asia, and Europe, as well as leading experts from relevant United Nations agencies, international research organizations, and academia.

Representatives from fourteen parliamentary assemblies participated, including the African Parliamentary Union (APU), Arab Inter-Parliamentary Union (Arab IPU), Arab Parliament, ASEAN Inter-Parliamentary Assembly (AIPA), Assemblée Parlementaire De La Francophonie (APF), European Parliament (EP), Inter-Parliamentary Assembly of Member Nations of the Commonwealth of Independent States (IPA CIS), Parliamentary Assembly of the Black Sea Economic Cooperation (PABSEC), Parliamentary Assembly of the Council of Europe (PACE), Parliamentary Assembly of the Mediterranean (PAM), Parliamentary Assembly of the Organization for Security and Cooperation in Europe (OSCE PA), Parliamentary Assembly of the Organization of Islamic Cooperation Member States (PUIC), Parliamentary Assembly of Turkic States (TURKPA), and Southern African Development Community Parliamentary Forum (SADC PF). Representatives from the Shura Council of the State of Qatar also took part.

The expert panel featured representatives from the United Nations Office on Drugs and Crime (UNODC), the UN Security Council Counter-Terrorism Committee Executive Directorate (CTED), the Chamber of Deputies of the Italian Parliament, the Italian National Cybersecurity Agency, and other international organizations and think tanks, such as [the Geneva Centre for Security Policy](#), [Mythos Labs](#), , [the Centre for Global Studies, the Parliamentary Assembly of the Mediterranean (PAM)](#), and [the Ad Hoc Committee on Countering Terrorism of the OSCE Parliamentary Assembly](#).

The Policy Dialogue comprised three main sessions:

1. Global and regional challenges and threats associated with the use of AI and other new technologies for terrorist purposes;

2. Good international and regional parliamentary practices on preventing and countering the use of AI and other new technologies for terrorist purposes;

3. International legal framework for preventing and countering the use of AI and other emerging technologies for terrorist purposes.

The Dialogue concluded with key recommendations on preventing and countering the use of AI and emerging technologies by terrorist and extremist organizations, emphasizing the critical roles of national parliaments and multilateral parliamentary assemblies in these efforts.

SESSION REPORTS

SESSION I. Global and regional challenges and threats, associated with the use of Artificial Intelligence (AI) and other new technologies for terrorist purposes

The session provided a comprehensive overview of current and emerging challenges to global and regional security arising from the misuse of AI and other emerging technologies for terrorist purposes. Participants emphasized the transformative impact of these technologies on the evolving nature of terrorism and their significant implications for the national security of Member States.

The discussion explored global threats associated with AI-driven tools, such as the creation and dissemination of disinformation, propaganda, and deepfakes, which are increasingly used for recruitment and radicalization. Concerns were also raised about the automation of attacks through AI-powered drones and autonomous systems. Cybersecurity vulnerabilities, particularly those exploited by AI-enhanced hacking techniques targeting critical infrastructure, were identified as pressing global issues.

At the regional level, participants highlighted disparities in technological capacity, which result in uneven abilities to detect and counter AI-enabled threats. Such disparities exacerbate the challenges of risk management, as social media algorithms often amplify localized grievances, fuelling polarization and extremism.

The national security implications of these threats were also underscored, with participants noting increasing risks to critical infrastructure, such as energy grids, financial systems, and communication networks. The sophistication of AI-driven evasion tactics was identified as a major challenge in the detection and mitigation of these threats.

Key points from the discussion included:

- **Dual Nature of AI**: AI presents both opportunities and risks, necessitating proper regulation by governments.

- **Rapid Technological Growth**: The exponential growth of these technologies often outpaces regulatory measures, leaving gaps in oversight.

- **Weaponization of AI**: Terrorist organizations are leveraging AI to produce and deploy weaponized drones and deepfakes in conflict zones. Emerging risks, such as deliberately corrupting AI systems (e.g., LLM poisoning), were also identified.

- **Exploitation for Propaganda and Recruitment**: AI is increasingly exploited by terrorist organizations to enhance propaganda and recruitment efforts, with significant advancements in leveraging new technologies for malicious purposes.

SESSION II. Good international and regional parliamentary practices on preventing and countering the use of AI and other new technologies for terrorist purposes

The session focused on showcasing effective international and regional parliamentary practices for preventing and countering the use of AI and other emerging technologies for terrorist purposes. It also aimed to identify actions necessary for implementing effective countermeasures while safeguarding technological progress and economic development. Additionally, the session explored ways parliamentarians and parliamentary assemblies can support these efforts at both the national and international levels.

The session featured a presentation by the Italian National Cybersecurity Agency (NCA), which addresses terrorism-related issues as part of its broader cybersecurity mandate. The NCA works on AI-related challenges within the framework of cybersecurity and prioritizes avoiding the mistakes made during the early development of the Internet. Currently, the agency emphasizes the importance of prioritizing security in emerging technologies to reduce vulnerabilities. It also strives to enhance inter-agency cooperation to devise effective responses to rapidly evolving challenges. Recognizing the immense power of these rapidly advancing technologies to produce both benefits and harm, the NCA is investing in forecasting their development to minimize potential security risks.

The OSCE PA's Resolution on "Artificial Intelligence and the Fight Against Terrorism" (adopted on 29 June 2024, in Bucharest, Romania) was a key theme of discussion during the Dialogue and recognized as one of the best international practices. The Resolution outlines a comprehensive framework for addressing the opportunities and risks posed by AI in counter-terrorism efforts. It emphasizes the need to combat terrorism and violent extremism while upholding human rights, fundamental freedoms, and the rule of law. Recognizing AI's potential to enhance security, the Resolution also addresses the risks of its misuse by terrorist organizations for activities such as planning, recruitment, and spreading propaganda. The Resolution calls for stronger legal frameworks and oversight mechanisms to regulate the development and use of AI, ensuring transparency, ethical compliance, and accountability. It highlights the importance of public-private partnerships to enforce transparency and mitigate risks, while promoting the use of AI tools to detect and counter terrorist activities. To foster societal resilience, the Resolution advocates for public education campaigns, particularly targeting youth, to enhance media literacy and counter online polarization. It also stresses the importance of mandatory labelling of AI-generated content to combat misinformation. International cooperation is underscored as a critical element, with the resolution encouraging states to exchange best practices and technical expertise through multilateral forums like the OSCE. By leveraging AI responsibly and collaboratively, the resolution provides a balanced approach to strengthening global counter-terrorism efforts while safeguarding human rights.

The PAM Centre for Global Studies (CGS) presented its recent report: "The Malicious Use of AI and Emerging Technologies by Terrorist and Criminal Groups: Impact on Security, Legislation, and Governance". The report explores how terrorist groups, transnational criminal networks, and

other non-state actors exploit new and emerging technologies. It examines the impact of these technologies on national and regional security, as well as their consequences for state institutions and processes, including cyber-attacks, misinformation, disinformation, political violence, hate-driven cultures, and systemic resilience. Additionally, the document assesses the current state of security-related regulatory frameworks at national and continental levels, highlighting areas for improvement. It is aligned with strategic directions drawn from resolutions, declarations, and reports by the United Nations and its affiliated organizations, as well as AI governance initiatives and legislation by Member States worldwide. The report offers a comprehensive set of strategic, technical, and policy-related recommendations, many of which emphasize the critical role of parliamentary responses. As a "living document," it is intended to be continuously monitored and updated to reflect evolving challenges and opportunities.

As part of its contribution to good international and regional parliamentary practices, the Inter-Parliamentary Assembly of Member Nations of the Commonwealth of Independent States (IPA CIS) provided an overview of its efforts in this field. In 2023, it adopted Recommendations on the regulatory framework for AI, including ethical standards for research and development, aiming to establish a unified system of legal and ethical norms that promote AI development across various economic sectors of CIS member states while ensuring the protection of citizens' rights and maintaining security. Currently, the IPA CIS is drafting a model law, *On Artificial Intelligence Technologies*, to regulate AI throughout its life cycle, aligning with the agendas of the United Nations General Assembly and the International Telecommunication Union. A key feature of this initiative is the integration of technological impact assessments into the legislative process to minimize risks and prevent negative consequences for humanity. Additionally, the IPA CIS is developing a model law, *On Countering the Use of Autonomous and Robotic Systems for Terrorist and Extremist Purposes*, recognizing the need to address security challenges posed by AI's rapid evolution. With autonomous and robotic systems becoming as commonplace as household appliances, this draft law seeks to counter criminal intent—whether from system developers, typically responsible for software design, or users seeking to exploit general-purpose systems for malicious purposes.

The experts and participants also discussed the European Parliament's Resolution on Artificial Intelligence in a Digital Age (adopted on May 3, 2022), which is one of the most comprehensive acts that examine and address the transformative impact of AI and its implications for terrorism, extremism, and security. The resolution highlights the critical role of AI in aiding law enforcement agencies in combating organized crime, terrorism, and cybercrime. High-risk sectors are identified as priorities for risk assessment to mitigate potential threats to security and fundamental rights. The misuse of AI in hybrid warfare and foreign interference is a significant concern, with the resolution emphasizing risks such as disinformation campaigns, economic destabilization, and election manipulation that could favor extremist groups or undermine democratic institutions. It also warns about the proliferation of deepfakes and AI-enabled identity theft, which undermine trust in digital content and exacerbate socio-political polarization. The Resolution reiterates the European Parliament's call for an international ban on lethal autonomous weapons systems

(LAWS) and stresses the necessity of meaningful human oversight in military AI applications to ensure adherence to legal and ethical principles. To address these challenges, the resolution emphasizes the need for robust, flexible, and future-proof regulatory frameworks that protect fundamental and human rights.

The participants also referenced the Inter-Parliamentary Union (IPU) Resolution titled "The Impact of Artificial Intelligence on Democracy, Human Rights, and the Rule of Law," adopted on 17 October 2024, highlighting its relevance to the counter-terrorism context. The resolution underscores the importance of parliaments taking an active role in shaping AI governance to ensure that technological advancements do not undermine democratic values, human rights, or the rule of law. Although it does not directly address terrorism, it raises critical concerns, such as AI's potential to facilitate the spread of misinformation, disinformation, and extremism—factors that can destabilize societies and fuel violent ideologies. The resolution also emphasizes the risk of AI amplifying biases and discrimination, including gender-based violence and online extremism, and calls for robust legal frameworks to ensure transparency and accountability in AI development and deployment. Furthermore, the resolution advocates for a human-centric approach to AI governance, urging measures to prevent the misuse of AI for surveillance, data manipulation, and the creation of harmful content, such as AI-generated deepfakes. It stresses the need for inclusive international cooperation to ensure AI technologies are used responsibly and equitably, protecting individual rights and fostering societal trust. Additionally, the resolution calls for parliaments to prioritize education and capacity-building on AI, ensuring that they are equipped to address the challenges posed by emerging technologies, including their potential impact on national security and counter-terrorism efforts.

The Council of Europe "Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law" was mentioned during the Dialogue, alongside other international instruments. Although it does not directly address issues related to terrorism, it is the first-ever international legally binding treaty on AI with specific focus on human rights, democracy and rule of law. The Convention aims to ensure that activities throughout the lifecycle of artificial intelligence systems align fully with human rights, democracy, and the rule of law while fostering technological progress and innovation. Additionally, it seeks to address any legal gaps that may arise from rapid technological advancements.

SESSION III. International legal framework for preventing and countering the use of AI and other emerging technologies for terrorist purposes

Building on previous sessions that addressed challenges, threats, and existing practices, the third session focused primarily on the work and recommendations of relevant UN entities, as well as international and regional organizations, in preventing and countering the use of AI and new technologies for terrorist purposes. The session also explored the support these organizations provide to Member States, including legislative bodies, in implementing UN Security Council resolutions and recommendations related to AI and new technologies.

The [Cybersecurity & New Technologies Unit of the United Nations Office of Counter-Terrorism / United Nations Counter-Terrorism Centre (UNOCT/UNCCT)](#) delivered a presentation on its efforts to strengthen the capacities of law enforcement and criminal justice authorities in selected partner countries to counter the exploitation of new and emerging technologies for terrorist purposes. The Unit also highlighted its work in supporting Member States in leveraging these technologies in the fight against terrorism. Additionally, the Unit showcased its series of publications on the Cybersecurity and New Technologies theme, which include:

- *Conducting Terrorist Threat Assessment: The Use of New Technologies for Terrorist Purposes;*

- *Designing National Counter-Terrorism Policy Responses to Counter the Use of New Technologies for Terrorist Purposes;*

- *Law Enforcement Capabilities Framework for New Technologies in Countering Terrorism;*

- *Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia;*

- *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes.*

The [Action against Terrorism Unit of the Organization for Security and Co-operation in Europe (OSCE)](#) shared its perspectives and experiences in preventing and countering the use of AI and new technologies for terrorist purposes. The Unit emphasized that its efforts are aligned with the recently adopted OSCE Resolution on AI and the Fight Against Terrorism. It highlighted the importance of engaging a broad range of non-governmental actors—including civil society, women, youth, businesses, industry, and media—in preventing violent extremism and radicalization that lead to terrorism (VERLT). The presentation also stressed the critical need to support these actors in leveraging AI to address challenges in preventing VERLT, while rigorously considering ethical implications, mitigating algorithmic biases, and safeguarding fundamental privacy and human rights.

The [Terrorism Prevention Branch of the United Nations Office on Drugs and Crime (UNODC TPB)](#) presented its work on promoting the responsible and ethical use of AI and advanced technologies to prevent and counter the misuse of online spaces by terrorists. The presentation emphasized that violent extremist and terrorist groups are increasingly exploiting the digital domain for activities such as propaganda, incitement, recruitment, and operational coordination. UNODC TPB referenced research indicating that these groups are experimenting with generative AI tools to enhance their propaganda strategies. This includes exploring capabilities such as media generation, automated multilingual translations, synthetic propaganda creation, variant recycling, personalized messaging, and bypassing moderation systems to amplify their reach. Additionally, UNODC underscored the recent adoption of [the United Nations Convention against Cybercrime](#), for which the UNODC served as the secretariat. This groundbreaking global treaty provides countries with essential measures to prevent and combat cybercrime while fostering enhanced international cooperation in sharing electronic evidence for serious criminal cases.

The [Security Council's Counter-Terrorism Committee (CTC) and the Counter-Terrorism Committee Executive Directorate (CTED)](#) delivered a presentation highlighting CTED's support to Member States in identifying innovative and collaborative approaches to address the misuse of ICT by terrorists. The presentation emphasized the development of technological solutions that harness the potential of ICT for positive purposes while respecting human rights, fundamental freedoms, and international legal obligations. CTED also shared insights on promoting and facilitating technical assistance and fostering public-private partnerships to counter the exploitation of digital technologies by terrorist groups. Additionally, CTED assists Member States in addressing terrorist narratives both online and offline, underlining the importance of balancing efforts to counter hate speech with safeguarding freedom of expression. The presentation stressed the need for States to collaborate in developing durable solutions to these challenges, emphasizing the importance of finding common ground despite differing perspectives. CTED provided critical recommendations on measures to prevent and counter the use of AI and emerging technologies for terrorist purposes. These recommendations included building the capacity of criminal justice systems to address ICT-based and AI-related crimes, enhancing accountability in the tech sector by ensuring companies take responsibility for practices that enable the misuse of their platforms—such as harmful algorithms, unmoderated spaces, and the sale of services to terrorist groups—and developing a global "minimum tech standard" for governments to effectively prevent and counter ICT-based terrorism.

RECOMMENDATIONS

The following recommendations were raised by the experts and participants during the Dialogue, which have been conveniently organized into seven thematic areas to address the challenges and opportunities posed by AI and emerging technologies in counter-terrorism.

1. Legislation and Policy Development
- Develop robust national legislation to regulate the use of AI and emerging technologies, ensuring it addresses dual-use concerns (both beneficial and harmful applications) to prevent misuse by terrorist groups.   - Enact and update laws to explicitly criminalize the misuse of AI and new technologies for criminal purposes, including terrorism.   - Harmonize legislation on AI and emerging technologies across countries to ensure consistency.   - Establish common standards for digital forensics and electronic evidence.   - Ensure that legislation and regulation are carefully balanced to avoid overregulation, which could hinder technological progress and development. Given the rapid pace at which technologies are evolving, legislation must remain flexible and adaptable, as traditional legal frameworks often struggle to keep up with innovation. This balance should be pursued through global cooperation and adherence to fundamental rights.
2. Human Rights and Data Protection

- Ensure counter-terrorism measures comply with human rights, prioritizing the protection of personal data and upholding justice, equality, and fairness.
- Implement efficient measures to safeguard data and personal information in a human rights-compliant manner.
- Address ethical implications, algorithmic biases, and fundamental privacy concerns when leveraging AI to counter terrorism.

3. Capacity Building for Law Enforcement and Justice Systems

- Equip and train law enforcement agencies to counter AI-driven terrorist and extremist activities effectively, ensuring alignment with international human rights standards.
- Build the capacity of criminal justice systems to address ICT-based and AI-related crimes.
- Provide comprehensive training and resources to prepare law enforcement agencies for challenges posed by emerging technologies.

4. Education and Public Awareness

- Prioritize investments in digital literacy and education to empower citizens, especially youth, to critically analyse information, recognize misinformation, and counter extremist propaganda.
- Integrate AI and emerging technologies into educational curricula to help individuals identify extremist content and understand its dangers.
- Support public education initiatives to build resilience against disinformation and propaganda campaigns driven by AI technologies.
- Promote public awareness initiatives, including media literacy and the labelling of AI-generated content, to combat misinformation.

5. International Cooperation and Partnerships

- Enhance international cooperation to address the transnational use of AI and new technologies for malicious purposes, promoting cross-border collaboration.
- Support the creation of an international security agency, such as "CyberPol", modelled on Interpol, to counter cybercrimes and terrorism globally.
- Facilitate cooperation between national authorities, regional bodies, and international organizations to share intelligence, best practices, and technological expertise.
- Encourage multilateral cooperation and increased public-private partnerships to promote transparency and accountability in counter-terrorism efforts.
- Promote cross-border collaboration to ensure effective and consistent efforts in countering terrorism and violent extremism.

6. Collaboration with the Tech Sector

- Promote close collaboration between governments, the ICT sector, and the tech industry to create safeguards that prevent the misuse of AI by terrorist organizations.
- Enhance accountability in the tech sector, ensuring companies take responsibility for practices enabling misuse, such as harmful algorithms, unmoderated spaces, and sales of services to terrorist groups.
- Develop a global "minimum tech standard" for governments to prevent and counter ICT-based terrorism effectively.
- Encourage collaboration with technology companies to enhance threat detection and mitigate risks associated with AI tools and platforms.

7. Role of Parliamentary Assemblies

- Leverage parliamentary assemblies to raise awareness, promote international standards, and advocate for technical assistance in counter-terrorism measures.
- Parliamentarians should lead efforts in facilitating and fostering international collaboration on counter-terrorism at all levels, ensuring national efforts align with international standards.

CONCLUSION AND FOLLOW-UP ACTIONS

The expert discussions and participant contributions during the dialogue highlighted the evolving challenges posed by AI and emerging technologies in counter-terrorism. Key recommendations emerged across several critical areas, including legislative development, human rights protections, law enforcement capacity-building, public education, international collaboration, and the role of parliamentary assemblies. These recommendations aim to ensure a balanced, coordinated, and human rights-compliant response to the opportunities and risks these technologies present in preventing and countering terrorism and violent extremism.

To advance the implementation of these recommendations, the UNOCT Programme Office on Parliamentary Engagement in Prevention and Countering Terrorism will continue to facilitate collaboration among parliamentary bodies, national governments, UN agencies, and other stakeholders. This ongoing coordination will support the development of strategies and policies that integrate AI and emerging technologies into counter-terrorism and PVE (preventing violent extremism) efforts, with a focus on capacity-building and technical assistance.

Looking ahead to 2025-2026, the UNOCT Programme Office on Parliamentary Engagement, in partnership with the UNOCT/UNCCT Cybersecurity & New Technologies Unit, will aim to organize a Global Parliamentary Conference on AI and emerging technologies. The conference will seek to serve as a platform for parliamentary dialogue, focusing on effective responses to the intersection of AI, new technologies, and counter-terrorism.

In addition, UNOCT will aim to organize a series of awareness-raising and capacity-building activities for parliamentarians and relevant staff from National Parliaments and partnering parliamentary assemblies. These activities will seek to enhance their understanding of AI and new technologies within the context of CT/PVE, enabling them to make informed, human rights-compliant decisions in their legislative and policy work.

Partnering parliamentary assemblies, particularly the participants of the Counter-Terrorism Coordination Mechanism for Parliamentary Assemblies, will be essential in implementing these initiatives. UNOCT will work closely with these assemblies to provide tailored support, expertise, and guidance to national parliaments, ensuring their active involvement in advancing efforts to counter terrorism.

Finally, the dissemination of expert recommendations will be prioritized to ensure that all relevant partners, stakeholders, and parliamentary assemblies align their efforts, fostering a coordinated global response to the challenges posed by emerging technologies in counter-terrorism.

The next (fifth) Parliamentary Policy Dialogue is scheduled for the second quarter of 2025, with the time, venue, and theme to be confirmed.

COMMUNICATIONS

Press releases

https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20241205_press_release_4th_policy_dialogue_rome.pdf

https://www.oscepa.org/en/news-a-media/press-releases/press-2024/under-osce-pa-leadership-legislators-from-across-the-globe-discuss-preventing-and-countering-the-use-of-ai-by-terrorists-at-policy-dialogue-in-rome

https://www.shura.qa/en/Pages/MediaCenter/News/07122024

https://pam.int/the-fourth-parliamentary-policy-dialogue/

https://turkpa.org/news/1766-turkpa-attended-6th-meeting-of-coordination-mechanism-for-parliamentary-assemblies-on-counter-terrorism-and-4th-parliamentary-policy-dialogue-organized-by-unoct

https://italyun.esteri.it/en/news/dalla_rappresentanza/2024/12/closing-remarks-delivered-by-permanent-representative-amb-maurizio-massari-at-fourth-parliamentary-policy-dialogue-on-countering-the-use-of-artificial-intelligence-and-new-technologies-for-terrorist/

Tweets

https://x.com/UN_OCT/status/1865127801377927552

https://x.com/oscepa/status/1864327102989734107