Background Guide for the United Nations General Assembly 1st (GA 1)

Committee Overview and Mandate

Introduction

The UN General Assembly, authorized by Chapter IV of the UN Charter, established six subsidiary committees in 1946 to address crucial matters related to peace, security, human rights, and development in specialized contexts.[1]

The 78th session of the United Nations General Assembly in 2023 prioritized accelerating action towards the 2030 Agenda and its 17 Sustainable Development Goals (SDGs).[2] Key events included the SDG Summit, High-level Dialogue on Financing for Development, Climate Ambition Summit, High-level Meetings on Pandemic Prevention, Universal Health Coverage, and the Fight against Tuberculosis, as well as the Preparatory Ministerial Meeting for the Summit of the Future and the commemoration of the International Day for the Total Elimination of Nuclear Weapons.[3] These topics represent the issues the body determined need further comprehensive debate and provide opportunities for interorganizational and interstate cooperation to advance peace, security, and sustainable development.

Governance, Mandate, Membership and Structure

Every UN Member State, as well as each Observer State, has a seat within the UNGA First Committee.[4] The President of the 78th session of the United Nations General Assembly, which took place from September 2023 to September 2024, was Dennis Francis of Trinidad and Tobago.[5] The General Assembly First Committee, or Disarmament and International Security (DISEC), addresses global security challenges, disarmament, and arms regulation within the UN Charter's scope.[6] It collaborates with the UN Disarmament Commission and the Conference on Disarmament to promote stability through reduced armaments.[7] As the only Main Committee with verbatim records, it alerts the Security Council to threats to international peace and recommends resolutions for adoption by the UNGA plenary session.[8]

---

[1] United Nations. "Charter of the United Nations". 1945
[2] UN General Assembly *High-level Week 2023*. https://www.un.org/en/high-level-week-2023
[3] Ibid.
[4] United Nations. "Membership of the Main Committees of the General Assembly." 2022. A/INF/77/2/Rev.1
[5] UN's *Dennis Francis of Trinidad and Tobago President of Seventy-Eighth General Assembly* (2023)
[6] United Nations General Assembly First Committee, https://www.un.org/en/ga/first/
[7] United Nations Office for Disarmament Affairs, https://www.un.org/disarmament/conference-on-disarmament/
[8] United Nations General Assembly First Committee, https://www.un.org/en/ga/first/

The First Committee of the UN General Assembly has two main subsidiary bodies: the Disarmament Commission (UNDC) and the Conference on Disarmament (CD).[9] The UNDC meets annually in New York for three weeks, focusing on two disarmament topics, one of which must include nuclear disarmament.[10] It reports to the General Assembly via the First Committee at least once a year. The CD, while not formally part of the UN, reports to the General Assembly and has its budget included in the UN's. It convenes triannually in Geneva, addressing issues such as nuclear disarmament, prevention of nuclear war and an arms race in outer space, assurances for non-nuclear-weapon States, new types of weapons of mass destruction, and transparency in armaments.

The First Committee of the UN General Assembly has been instrumental in shaping the global disarmament and international security agenda. Two landmark resolutions stand out in its history. Resolution 1 (I), adopted on January 24, 1946, in London, was the very first General Assembly resolution.[11] It established a Commission to address the challenges posed by the discovery of atomic energy. Another significant milestone was Resolution 1378 (XIV), which was co-sponsored by all Member States at the time, demonstrating a rare consensus on disarmament matters.[12] These resolutions highlight the First Committee's crucial role in tackling some of the most pressing security issues facing the international community.

Crime, Terrorism, and Warfare in Cyberspace

Background

The rapid digitalization and increasing use of social media presents both opportunities and challenges. While digital technologies can be leveraged for development, freedom of expression, political participation, and civic action, they can also be exploited by terrorists and violent extremists to spread hateful ideologies, recruit new members, and manage online communities. As the United Nations Secretary-General António Guterres stated in his *2018 Strategy on New Technologies*, while AI can have a profound positive impact on various sectors of society, it also poses risks and has the potential to obstruct the enjoyment of human rights and fundamental freedoms, particularly the rights to privacy, freedom of thought and expression, and non-discrimination.[13]

In *the United Nations Global-Counter Terrorism Strategy* (A/RES/60/288), Member States agreed to collaborate with the United Nations to find ways to coordinate international and regional efforts to combat terrorism on the Internet in all its forms, while also using the Internet as a tool to counter

[9] United Nations General Assembly First Committee, https://www.un.org/en/ga/first/
[10] United Nations Office for Disarmament Affairs, https://www.un.org/disarmament/institutions/disarmament-commission/
[11] United Nations General Assembly First Committee, https://www.un.org/en/ga/first/
[12] Ibid.
[13] UN Secretary-General's *Strategy on New Technologies* (2018) https://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies.pdf

the spread of terrorism.[14] *INSIKT Intelligence*, a tech startup, uses machine learning, natural language processing (NLP), and social network analysis (SNA) on open-source data from social media to identify potential online threats, dangerous content, and patterns of relationships between individuals or organizations.[15] This allows law enforcement to prioritize resources on potential threats while complying with data protection principles through data anonymization or pseudonymization. Data anonymization or pseudonymization also enhances compliance with data protection principles, such as those included in *the ASEAN Framework on Personal Data Protection or the Privacy Framework of the Asia-Pacific Economic Cooperation*.[16]

Artificial Intelligence

The global AI market is expected to surpass $100 billion by 2025, with AI-enabled systems supporting various sectors.[17] Terrorists, known for rapidly adopting emerging and under-regulated technologies, are likely to exploit AI as well. Given the cross-border implications of technological systems, a regional and international approach is crucial to prevent terrorists from exploiting regulatory gaps and vulnerabilities in AI systems. Building resilient governing structures is essential to respond to and mitigate the impact of the malicious use of AI by terrorists quickly and effectively. A survey by UNICRI and INTERPOL at the Third Annual Global Meeting on AI for Law Enforcement revealed that AI adoption in law enforcement is still in its early stages. Out of 50 representatives from law enforcement agencies worldwide, half considered their organization's AI knowledge and expertise to be "rudimentary", while 30% deemed it "intermediary", and only 20% regarded it as "advanced".[18]

Facial recognition, an AI-powered biometric technology, has seen a dramatic increase in adoption by law enforcement agencies worldwide, offering promise in analyzing video footage to identify persons of interest. The German Federal Police and INTERPOL have experimented with this technology, confirming its potential to identify relevant subjects in crowded places.[19] However, the rising use of facial recognition has also raised concerns among human rights groups and civil society organizations about the potential for the technology to reflect and reinforce pre-existing biases in law enforcement.

Terrorist groups have been exploiting AI-related technologies, particularly unmanned aerial systems or "drones", even though they have not been observed using AI directly. Drones are considered an AI-related technology because they can have varying levels of autonomy, such as

---

[14] The United Nations *Global Counter-Terrorism Strategy*, A/RES/60/288. https://undocs.org/en/A/RES/60/288
[15] INSIKT Intelligence, https://www.insiktintelligence.com/
[16] APEC *Privacy Framework* (2015)
[17] UN's *Weighing Benefits, Risks of Digital Revolution, Speakers in General Assembly Urge Action, Regulation to Ensure Technology Facilitates Development, Not Inequality* (2023)
[18] INTERPOL & UNICRI's Report *Towards Responsible AI Innovation: Second INTERPOL-UNICRI Report on Artificial Intelligence for Law* (2020)
[19] INTERPOL's *Facial Recognition* (2018) https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition

GNSS-supported flight stabilization and "sense and avoid" features, even when manually operated.[20] AI could potentially be used to provide even greater autonomy to these systems.

UNICRI's Centre for Artificial Intelligence and Robotics and the UN Counter-Terrorism Centre (UNCCT) of the UN Office of Counter-Terrorism (UNOCT) collaborated on a research initiative exploring the dual nature of AI in counter-terrorism, focusing on its potential malicious use by terrorists and its application in combating terrorist use of the Internet and social media.[21] This resulted in two reports: *"Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes"* and *"Countering terrorism online with artificial intelligence – An Overview for Law Enforcement and Counter-Terrorism Agencies in South and South-East Asia".*

Cybercrime

Cybercrime, a growing form of transnational crime involving organized crime groups, has turned the Internet into a platform for spreading hate speech, violent extremism, and pandemic misinformation. In 2019, over 7,000 data breaches exposed more than 15 billion records, with the cost expected to exceed $5 trillion by 2024.[22] During COVID-19 lockdowns, while the Internet became crucial for education and work, cyberbullying and digital violence made it hostile for many, particularly women. A UNICEF and UN SRSG poll revealed that one in three young people in 30 countries have experienced online bullying, with one in five skipping school as a result.[23]

The World Economic Forum launched *the Partnership against Cybercrime (PAC)* in 2020 to foster public-private collaboration in combating cybercrime.[24] The PAC serves as a platform for sharing insights and exploring approaches to drive effective cooperation against cybercrime, bringing together global businesses, leading law enforcement agencies, and prominent not-for-profit organizations. In January 2023, the PAC's efforts led to the establishment of *the Cybercrime Atlas* initiative, which aims to map and enhance the understanding of the cybercriminal ecosystem.[25]

The Global Program on Cybercrime, which aimed at assisting Member States in their efforts to prevent and combat cybercrime through capacity building and technical assistance, was established under the framework of *the UNODC's Thematic Program on Crime Prevention and Criminal Justice Reform* for the period 2012-2015.[26] The program has also been actively involved in supporting the implementation of *the United Nations Convention against Transnational*

[20] UNCCT's Report *Algorithms and Terrorism* (2021)
[21] UNICRI's Report *Countering Terrorism Online With Artificial Intelligence* (2021)
[22] UNDESA's Report *As Internet user numbers swell due to pandemic, UN Forum discusses measures to improve safety of cyberspace* (2023)
[23] UNICEF poll *More than a third of young people in 30 countries report being a victim of online bullying* (2019)
[24] The World Economic Forum *Partnership against Cybercrime* (2023)
[25] Ibid.
[26] The UNODC Global Program on Cybercrime
https://www.unodc.org/unodc/en/cybercrime/our-mandate

Organized Crime (UNTOC) and its Protocols, as well as other relevant international instruments related to cybercrime.[27]

Countering Violent Extremism

The Counter-Terrorism Committee has provided guidance for Member States through *the 2015 Madrid Guiding Principles* and *2018 Addendum on FTFs*, focusing on monitoring terrorist content online, reviewing mutual legal assistance laws for digital data requests, and gathering digital evidence.[28] CTED's work on ICT involves assessing Member States' implementation of relevant resolutions, promoting industry self-regulation and public-private partnerships, strengthening international cooperation for legal access to digital content, and promoting counter-messaging techniques.

Over two years, Facebook removed more than 26 million pieces of content from groups such as the Islamic State of Iraq and the Levant (ISIL) and Al-Qaida, which have proven adept at using the Internet and social media to communicate, spread their messages, raise funds, recruit supporters, inspire and coordinate attacks, and target vulnerable individuals.[29] A 2017 study found that there were approximately 23 million bots on Twitter, 140 million on Facebook, and 27 million on Instagram, with groups like ISIL skillfully using these bots to automatically spread their propaganda on social media platforms.[30]

The UN Office of Counter-Terrorism (UNOCT) has launched several initiatives focusing on cybersecurity and new technologies. The UNOCT/UNCCT *Cybersecurity and New Technologies* program aims to enhance the capacities of Member States and private organizations to prevent and mitigate the impact of terrorist cyber-attacks against critical infrastructure, as well as to recover and restore targeted systems in the event of such attacks.[31] In 2022, UNOCT/UNCCT and INTERPOL launched *the CT TECH* initiative, funded by the European Union and implemented under the UNCCT *Global Counter-Terrorism Program on Cybersecurity and New Technologies*.[32] CT TECH focuses on strengthening 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, while also supporting Member States in leveraging these technologies in the fight against terrorism.

The Counter-Terrorism Committee Executive Directorate (CTED) has been a key partner of the *Global Internet Forum to Counter Terrorism (GIFCT)*, an independent NGO founded by

---

[27] Ibid.
[28] United Nations Security Council Counter-Terrorism Committee *Security Council Guiding Principles on Foreign Terrorist Fighters: The 2015 Madrid Guiding Principles + 2018 Addendum* (2019)
[29] UNICRI's *Countering Terrorism Online With Artificial Intelligence* (2021)
[30] Ibid.
[31] UNOCT's *Cybersecurity and New Technologies*
https://www.un.org/counterterrorism/cybersecurity
[32] Ibid.

Facebook, Google, Microsoft, and Twitter in 2017.[33] CTED serves as a permanent observer to the GIFCT Independent Advisory Committee and its working groups on Academic and Practical Research and Legal Frameworks (Data). *Tech Against Terrorism* collaborates closely with GIFCT to support small platforms and develop technological solutions.

Conclusion

Delegates should focus their research on these three subsections: artificial intelligence, cybercrime, countering violent extremism. By exploring the challenges and opportunities presented by AI in the context of counter-terrorism efforts, delegates can develop comprehensive resolutions that promote the responsible use of AI while mitigating its potential risks. Through their research and recommendations, delegates have the opportunity to shape a more secure digital future for all.

Questions to Consider

How can Member States effectively balance the need for counter-terrorism measures in cyberspace with the protection of fundamental human rights?

How can the UN and Member States promote sharing of best practices in AI and counter-terrorism to prevent violent extremism online?

How can the UN and Member States foster multi-stakeholder partnerships to develop responsible AI for counter-terrorism?

What international frameworks can address the transnational nature of cybercrime and prevent exploitation by terrorist groups?

What initiatives can support Member States in strengthening cybersecurity and countering the use of emerging technologies by terrorists?

Helpful Links

1. https://www.un.org/en/ga/78/meetings/
2. https://unicri.it/Publications/Countering-Terrorism-Online-with-Artificial-Intelligence-%20SouthAsia-South-EastAsia
3. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf
4. https://aiforgood.itu.int/about-ai-for-good/un-ai-actions/
5. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2022-PDF-E.pdf

[33] CTED's Report *CTED Trends Alert: Member States Concerned by the Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism* (2021)

6. https://www.un.org/counterterrorism/cybersecurity#:~:text=In%202022%2C%20UNOCT%2FUNCCT%20and,supporting%20Member%20States%20in%20leveraging

7. https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity