BACKGROUND Guide

UNITED NATIONS
SECURITY COUNCIL

Table of Contents

Letter from the Dais.....3

Introduction to the Committee.....4

Veto Powers.....6

Introduction to the Agenda.....7

Key Issues.....9

Major Stakeholders.....12

Attempted Solutions.....14

Questions A Resolution Must Answer.....16

Bibliography.....17

Addressing the Threat to International Security Posed by the Misuse of Advanced Technology & Artificial Intelligence (A.I)

Letter from the Dais

Respected Delegates,

We have great pleasure in introducing you to the esteemed United Nations Security Council at OOBMUN26. Getting yourself a seat here isn't an easy task, this shows your well-earned experience, commitment, and past successes within the Model UN community. This is the highest level of debate imaginable, which sets a gold standard when it comes to professional etiquette, creative problem-solving, and impressive oratory skills. Though joining this committee is a testament to your unique abilities as a delegate, excelling in such conditions is something only extraordinary delegates can do.

Entering the international arena in these times of transformation, marked by new geopolitical trends, fast technological revolution, and constant cultural shifts that shatter any framework for the future, means that every day brings new complex headline stories that challenge our perceptions of stability and order of the international community. In order to take control of the direction our world will be moving in the hands of future policymakers, you need to get immersed into the demanding environment that a Security Council is capable of offering.

As your Executive Board, our aim is to go beyond mere rhetoric and see what your full diplomatic potential can be. We will demand that you prepare forward-thinking, implementable resolutions, negotiate across seemingly insurmountable ideological differences, and reach lasting agreement with conflicting states under strict deadlines. We plan on making sure that this committee gives you the true taste of the practice of real world diplomacy, that you feel its painful friction and deadlocks but gain the resolve that solutions can yet be found through endless negotiations. More than anything else, we strive to create an invigorating atmosphere that will make your participation at this conference memorable.

Warm regards,

President – Aman Ahmed

President – Ryan Jo Rajesh

Introduction to committee

United Nations Security Council (UNSC)

The United Nations Security Council serves as a primary body of the United Nations, with the objective of fostering peace and stability globally. Since 1945, the Security Council has been the origin of many achievements, some of which include providing security, responding during crisis situations, and giving their overall support.

Structure of the UNSC:

The Council constitutes 15 member states, including 5 permanent members (China, United States, Russia, United Kingdom and France).

Permanent membership grants a country the right to veto (veto power explained below) and table resolutions.

Powers and Functions:

Imposing Sanctions: The Council can impose economic sanctions, arms embargoes, or travel bans on countries violating international law. Authorizing

Military Action: This is the most significant power. The Council can authorize the use of force, including deploying peacekeeping missions.

Admission of New Members: The Council recommends to the General Assembly which states should become UN members.

Recommending the Secretary-General: The Council recommends candidates for the position of UN Secretary-General to the General Assemble

The UNSC is the only UN body where resolutions are binding legally on all member states. The Charter grants the UNSC the unique right to form decisions that all member states are required to comply with.

However, binding does not guarantee compliance, as enforcement depends on:

1.Political Will: The commitment from institutions and key leaders to enact, prioritize and enforce specific policies or reforms considering facing the burden of costs or opposition.

2. Alignment Among Major Powers: Countries forming closer ties in various aspects such as economically, politically and militarily. On the basis of shared interests.

3.Willingness to Commit Resources: Being prepared and ready for the allocation of assets at any given time such as money, people, time or equipment that would impact a project, cause, a specific goal.

It is made clear that decision-making is shaped by alliances formed to ensure compliance among member states, prevent conflicting decisions, and create leverage. Such leverage arises when certain countries face limiting factors that others do not, allowing non-limiting advantages to be strategically exercised. Veto threats must also be taken into account before any decision is made. Consensus among member states is frequently achieved not through adherence to core values or long-term objectives, but through political maneuvering, pragmatic compromises, or settling for the least objectionable option in order to move forward. United Nations Security Council (UNSC)

Delegates are therefore expected to think and maneuver strategically within these constraints, as feasibility is often the determining factor and is more likely to lead to a successful outcome. Implicitly, the failure of a resolution to pass should itself be understood as a political outcome.

VETO Powers

UNSC outcomes are usually decided before a resolution paper is put upon a vote, as formal voting is the final procedural step and not the decision point. By the time a resolution has reached voting procedures, its fate is often already clear. This occurs during informal negotiations where signals of veto are exchanged between member states and veto members, determining whether a resolution is even worth tabling. As a result, many drafts never reach the floor due to the anticipation of vetoes.

When veto members signal red lines by expressing concerns regarding specific resolutions, these "red lines" usually relate to:

1.Authorization of force

2.Condemning or explicitly naming specific member states or actors

3.Language that would impact and affect intervention or sovereignty

These red lines are typically communicated indirectly, with concerns framed diplomatically rather than as explicit veto threats. However, such signaling can escalate into threats where a veto member withholds support until changes satisfying their position are made. Even a single veto threat can cease negotiations entirely; therefore, delegates must account for veto risk even when it is not explicitly stated, ensuring that P5 members can comply with the resolution.

Veto threats disproportionately affect resolution sponsors. Smaller states often co-sponsor resolutions to gain political protection, while P5 members selectively select sponsors to avoid the risk of public defeat. Consequently, UNSC decision- making is driven more by anticipation than confrontation, with avoiding a veto frequently prioritized overachieving maximal outcomes.

Veto power shapes every stage of UNSC decision-making. Delegates are expected to anticipate objections early, prioritize enforceable compromises, and avoid language likely to trigger a veto. As such, veto power should be

treated as a central point of negotiation skill, demanding strategic thinking and realism in UNSC diplomacy.

Introduction to the agenda

The current international system is poised at a crucial structural inflection point. The extremely rapid development and merging of cutting-edge technologies such as artificial intelligence (AI), machine learning systems, autonomous programs, quantum computers, and synthetic biology have significantly altered the dynamics of global security, diplomacy, and stability. While traditional weapons have been limited by their physical/material restrictions, time requirements for industrial production, and geographical considerations, cutting-edge digital technologies work at near-light speed in an unrestricted electronic space.

Traditional multilateral security arrangements were established on the basis of the fundamental principles of deterrence, arms control, transparency, and state identification. The existence of highly developed and multi-purpose artificial intelligence contradicts these principles in every possible way. Models, agents, and hyper-fast decision-making algorithms work through high-dimensional parameter space that is largely opaque in its functioning, introducing uncertainty to the processes of military command, conflict escalation control, and supervision of critical civilian infrastructure.

This problem lies at the heart of the current policy agenda. The same scientific breakthroughs that fuel the development of machine learning algorithms used in medical research into cancer, climate studies, logistics, and economics forecasting can just as easily – without much additional programming effort – be applied to building synthetic viruses, creating zero-day cyber-attacks, spreading hyper-personalized propaganda or conducting autonomous physical strikes. In that the research into advanced AI mostly uses commercial off-the shelf hardware and private funding through open-source code repositories, the traditional line between military procurement and commercial business has been effectively erased.

In addition, the introduction of AI into strategic defense plans carries the risk of shrinking decision-making timelines. Being in a hurry to keep up with other states in the competition for tactical superiority, one would need to transfer more and more responsibility to decision support software and even automatic execution of certain actions, thus increasing the danger of “flash wars. ”

There is also the need for the international community to counter the structural inequalities that are inherent in the unequal availability of computing infrastructures, semiconductor manufacturing, specialized knowledge about algorithms, and quality data used for training. The fact that the development of new frontier technologies takes place among only a few technologically advanced nations and companies is a dangerous situation that could lead to the emergence of a hegemony of technology. Developing countries are likely to be affected by the security externalities as well as disruptions to society resulting from misuse of algorithms without being equally involved in the formation of international norms, technical standards, or regulation.

Therefore, there is the need for a solution to the challenge posed by misuse of advanced technology and AI to take the form of a multilateral approach. Such an approach will involve balancing two goals – protecting international peace through ensuring that there are robust and verifiable measures that respect IHL and human rights while preventing digital protectionism at the same time.

Key Issues

A. Lethal Autonomous Weapons Systems (LAWS) and AI Military Integration

The introduction and possible implementation of Lethal Autonomous Weapons Systems (LAWS), which can be defined as weapons systems that are able to select and attack targets autonomously without human involvement, pose a revolution of sorts in the concept of warfare. The central issue of legality and ethics is connected with the adherence to the principles of International Humanitarian Law (IHL), namely the principle of distinction, proportionality, and military necessity. Algorithms operate through statistical pattern recognition gained in the process of training; they lack human qualities of discernment and reasoning.

B. Proliferation to Non-State Armed Actors and Malicious Actors

The quick proliferation of sophisticated foundation models, which are readily accessible to the general public through an open-source approach, decreases the cost associated with executing any operation by non-state armed actors, violent extremists, and transnational organized crime organizations. There is no need for special lab setups or academic degrees in order to perform a variety of tasks.

Biological Security and Chemical Threats: The tools that are used to generate designs based on molecular biology and protein folding can be reprogrammed to create toxic chemicals and biological organisms, which would not be detectable and could withstand vaccination.

Asymmetric Kinetic Attacks: Non-state armed actors may use available hardware and open-source computer vision tools to build completely autonomous IEDs and loitering munitions, which could function without a GPS connection and in the absence of communication.

Automated Illicit Financing: Complex laundering schemes can be automated using sophisticated algorithms that are designed for DeFi systems.

C. Offensives Cyber Capabilities with Artificial Intelligence and Vulnerability in Critical Infrastructure

Artificial intelligence and cyber war together make up a very effective force multiplier when it comes to offense capabilities. The targets of the offensives include civilian critical infrastructure such as nuclear power stations, electric power systems, automated water distribution systems, transaction clearinghouses, and telecommunications systems. Because of the rapidity and decentralized nature of the automated attack, pinpointing an accurate attribution is very hard. The malicious attacker may use signature spoofing or route attacks across multiple jurisdictions, thus making deterrence theory ineffective and making misretaliations possible.

D. Information Warfare, Deepfakes, and Cognitive Security

The use of highly realistic digital images through the creation of deepfake video, synthesized audio streams, and advanced natural language systems has brought about a new battlefield environment. Cognitive security, which refers to the safeguarding of the information environment from deliberate manipulation, is crucial for national and global security.

Political and Electoral Manipulation: Micro-targeted information campaigns powered by adaptive language systems can be used in large numbers to influence public debate, cause civil disturbance, and damage the credibility of democratic structures.

Crisis Disruption: In times of war and natural disasters, synthetic media can create a false message of capitulation, false leadership messages, and a state of public emergency to paralyze the government control mechanisms and disturb the general population.

route attacks across multiple jurisdictions, thus making deterrence theory ineffective and making misretaliations possible. D. Information Warfare, Deepfakes, and Cognitive Security C. Offensives Cyber Capabilities with Artificial Intelligence and Vulnerability in Critical

E. Structural Inequalities and the "AI Divide"

Support structures of cutting-edge artificial intelligence in terms of hardware, computing resources, and research capacity are extremely concentrated in a limited number of economically developed countries and multinational tech companies. Cutting-edge models need specialized high-end semiconductors, vast electricity grids, advanced cooling systems, and big data sets.

This results in huge inequalities between nations:

Exclusion from Governance: Developing countries are often not included in closed technical and regulatory discussions, which means that resulting international agreements are in line with the strategic interests of major tech players.

Vulnerability: Countries which do not have AI verification and defense mechanisms become laboratories or targets for advanced algorithmic manipulation and cyber exploitation.

Economic Dependence: Lack of access to advanced computing facilities leads to economic dependence, forming new neocolonial relationships, when developing nations provide raw data and use proprietary algorithms.

Major Stakeholders

1. United States of America

Since it is the home base of many frontier AI companies such as Microsoft, Meta, Anthropic, and OpenAI, the country prefers national and industry-driven, capitalism-oriented methods when it comes to regulating AI rather than adopting binding regulations for all.

In 2025, it turned down the international organizations' attempts to establish centralized control and global governance over AI, choosing instead voluntary safety pledges, evaluations initiated by the industry, and flexible national standards.anctions and export restrictions were imposed that strictly prohibited the export of GPUs, chips, and RAM to countries such as China and Russia in order to maintain technological and strategic leverage.

In the area of multilateral leadership, you led the adoption of UNGA resolution 78/265 (2024), which established an international standard for safe, secure and trustworthy AI systems le development. The Political Declaration on the Responsible Military Use of AI and Autonomy was launched (in 2023), promoting non-binding international norms which require explicit human oversight, thorough testing, and transparent operational practices in military applications.

2. China

It is the main technological power with a state-controlled digital ecosystem, the country prefers multilateral governance centered on the UN to coalitions led by the West while promoting state control and technological independence. The UN-Centric approach to global governance supported the Global AI Governance Initiative (2023) and the Global AI Governance Action Plan (2025), advocating for the establishment of a central international governance body operating within the UN framework to take the place of the informal western-led alliances.

The firm firmly opposes the Western export controls and the sanctions on GPUs and chips, describing them as unilateral technological embargoes and examples of digital hegemonism which disturb global supply chains. The Global South should be supported in building its capacity by obtaining

technology transfers, sharing computing infrastructure, and gaining cross border digital access in order to avoid the global intelligence gap widening.

3. Russian Federation

It places a high priority on asymmetric strategic capabilities as a major military power, the country prefers absolute national command sovereignty to international legal restrictions or systems of supervisory oversight. The idea that current International Humanitarian Law (IHL) and the UN Charter are entirely adequate for regulating military AI is put forward, in this way preventing any attempts to reach new legally binding agreements or treaties banning autonomous weapons.

Opposition to External Oversight: It rejects all international verification mechanisms, technical inspections, or hardware auditing systems which could jeopardize national defense software or sovereignty. In regard to Strategic Autonomy, the country voted against the United Nations General Assembly resolutions which aimed at establishing external supervisory bodies for AI that were led by civil society or supported by the West, in order to safeguard its own domestic research and the flexibility in the deployment of military AI.

4. European Union

The bloc, being a powerful regulatory force that stresses human rights and ethical protections, prefers legally binding, risk-oriented legislative minimum standards to market-based self-regulation. The legislative framework has been enacted in the form of the EU AI Act, which creates the world's first all-encompassing and legally binding system based on risk levels and requires a high degree of transparency from the use of high-risk AI while also prohibiting applications that are unacceptable such as social scoring.

There is a two-level stance on autonomy: that of advocating for a clear legal distinction between autonomous weapons which operate beyond human oversight and automated defensive systems which are permitted, such as air defense networks. International harmonization is achieved by means of the European AI Safety Institutes and through minilateral initiatives such as the G7 Hiroshima AI Process in order to standardize pre-deployment evaluations and red-teaming protocols.

5. Non-Aligned Movement

As a group representing the Global South, the bloc supports inclusive governance led by the United Nations and fair access to technological resources rather than closed agreements made by the major technology companies.

The demand for equitable access holds that any global regime for AI governance must contain binding commitments regarding the transfer of technology, financing of computing infrastructure, and the building of technical capacity in order to avoid digital neo-colonialism.

Universal multilateralism opposes regulatory coalitions that are made up solely by the major powers and insists that all global standards and regulatory rules should be negotiated in the universal UN forums.

In favour of binding arms control: strongly supports internationally binding instruments for banning or strictly regulating Lethal Autonomous Weapons Systems (LAWS), on the grounds that developing countries would otherwise end up as testing sites for automated warfare without having equivalent defensive capabilities

Attempted Solutions

1.UNGA Resolutions 78/265 and 78/311 (2024):

GA 78/265 resolution (March 2024): First of a series of nonbinding global guidelines for development of "safe, secure, and trustworthy" AI technologies aligned with human rights and civil liberties-adopted in consensus at the UN General Assembly and led by the US.

Resolution GA 78/311 (July 2024): Led by the United States but with the backing of China, this continued resolution sought to bridge the global AI gap by fostering global cooperation and developing AI skills in developing countries.

2.Global Digital Compact & UN Governance Panel (September 2024):

Global Digital Compact which included a set of global principles for inclusive digital governance, of safety from harm from automation and for universal digital access. Independent Scientific Panel & Global Dialogue: This body was established by the UN General Assembly to carry out independent scientific evaluations of risks associated with emerging dual-use AI technologies.

3. Council of Europe Artificial Intelligence Convention (2024):

The first legally binding international treaty for AI, establishing compulsory legal requirements for human rights impact assessments, and concrete restrictions on AI uses for surveillance and law enforcement and public security.

4. UNIDIR Center of Excellence on AI, Peace and Security (2026):

This international platform, initiated by the UN Institute for Disarmament Research (UNIDIR), is designed to facilitate dialogue among all relevant strategic actors to reduce the risks associated with integrating artificial intelligence into early-warning systems, autonomous targeting and nuclear command and control.

5. REAIM Summits (2023 The Hague, 2024 Seoul):

Global summits at the level of governments, technology companies and defense analysts, to define a "Blueprint for Action" for the military use of AI.

Worked on defining voluntary red-teaming practices, mandatory human-in-the-loop, and crisis alerts to mitigate accidental algorithmic escalation.

6. CCW Group of Governmental Experts (GGE) on LAWS, Geneva:

Despite the existence of the UN Convention on Certain Conventional Weapons (CCW), where a GGE has been discussing the issue of autonomous weapons systems since 2014, only 11 non-binding guidelines on compliance with International Humanitarian Law (IHL) have been agreed upon. Negotiations toward a legally binding prohibition have yet to move forward owing to CCW consensus rules enabling states to block treaty negotiations.

7. Multilateral Export Controls and Compute Tracking:

The unilateral measures taken by big tech (targeted chip export controls, GPU monitoring, supply chain restrictions to hardware) served to prevent state-actors and strategic rivals from building rogue AI models and designs of viruses.

Questions a Resolution Must Answer

What strategy can the UN use to establish standards for definitions of the likes of autonomous targeting, meaningful human control and frontier dual use models?

What legal limitations and bans should be imposed on autonomous systems?

For example, should they be prohibited from using specific weapons or targeted at certain objects?

Is there an international auditor or verifier able to undertake an independent audit on compliance against the AI safety baselines without trading away state sovereignty and corporate privacy?

Are there any hardware-tracking or export control policies in place which could inhibit the weaponization of dual-use AI by non-state actors to weaponize biological and/or chemical weapons?

How will coordinated capacity-building and compute-transfer programs lead to a safe AI infrastructure and a seat at the table in AI governance for Global South countries?

What emergency "hotlines" and early-warning communication channels should major military powers put in place to prevent accidental escalation due to algorithm-induced errors?

Bibliography

Council of Europe. (2024). Framework convention on artificial intelligence and human rights, democracy and the rule of law (CETS No. 225). Council of Europe Treaty Series. https://rm.coe.int/1680afae3c

International Committee of the Red Cross. (2021). ICRC position on autonomous weapon systems: ICRC calls for new legally binding rules. ICRC Publications. https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems United Nations High-Level Advisory Body on Artificial Intelligence. (2024). Governing AI for humanity: Final report.

United Nations Secretariat. https://www.un.org/en/ai-advisory-body United Nations Secretary-General. (2023). Our common agenda: Policy brief 9 - A new agenda for peace (A/77/CRP.1/Add.8). United Nations. https://undocs.org/A/77/CRP.1/Add.8

Wagman, S., & Hubbard, S. (2025, April 8). Weaponized AI: A new era of threats and how we can counter it. Ash Center for Democratic Governance and Innovation, Harvard Kennedy School. https://ash.harvard.edu/articles/weaponized-ai-a-new-eraof-threats/

Puscas, I. (2023, October 12). AI and international security: Understanding the risks and paving the path for confidencebuilding measures. United Nations Institute for Disarmament Research (UNIDIR). https://unidir.org/publication/ai-andinternational-security-understanding-the-risks-and-paving-the-path-for-confidence-building-measures/

Boulanin, V., Palayer, J., & Ovink, C. (2025, November). Addressing the risks that civilian AI poses to international peace and security: The role of responsible innovation. Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/publications/2025/other-publications/addressing-risks-civilian-ai-poses-international-peace-and-securityrole-responsible-innovation

Nichols, M., Irish, J., & Rozen, C. (2026, September 23). AI leaders brief UN amid warnings technology could slip beyond human control. Reuters. https://www.reuters.com/business/ai-leaders-brief-un-amid-warnings-technology-could-slip-beyondhuman-control-2026-09-23/

Bazarkina, D. Y., & Pashentsev, E. N. (2019). Artificial intelligence and new threats to international psychological security. Russia in Global Affairs, 17(1), 147–170. https://doi.org/10.31278/1810-6374-2019-17-1-147-170

Esmailzadeh, Y., & Motaghi, E. (2024). International terrorism and social threats of artificial intelligence. Journal of Globalization Studies, 15(1), Article 3714231. https://doi.org/10.30884/jogs/2024.01.09



BACKGROUND *Guide*

UNITED NATIONS
SECURITY COUNCIL