2023

Jamia Millia Islamia
Model United Nations

United Nations General Assembly

JMI Model United Nations, 2023

Letter from the Executive Board

Dear Delegates,

Welcome to Jamia Millia Islamia Model United Nations 2023 and the United Nations General Assembly!

We are more than happy to be able to simulate one of the most significant committees existing in the contemporary world to discuss one of the most pressing global issues.

As your chairs, we promise to do our best to bring you a fruitful and efficient committee simulation.

We believe that you are resilient delegates who will be making the most out of your experience here and, most importantly, have fun while doing just that!

Please keep in mind that we are discussing a very crucial issue in our world today and it requires your utmost care and dedication. Remember that you are the leaders of the future!

Research as much as you can to be able to write the best possible resolution you can throughout the conference.

We believe in your abilities, and we crave to meet you soon!

All the best,
The Executive Board

Aryan Singh
Chairperson

Shreyash Dube
Vice Chairperson

Introduction to the Committee

The United Nations General Assembly (UNGA), also known as the 'Town Hall of the World', is the largest and most representative organ of the UN system. All UN Member States are represented in the General Assembly with each member state having one vote. Decisions on key issues such as international peace and security, admitting new members and the UN budget are decided by a two-thirds majority while other issues are decided by a simple majority. Many decisions are reached by consensus without a formal voting process.

As per the provisions of the UN Charter, the functions and powers of the General Assembly (GA) are:

- Discussing questions relating to international peace and security (except when a dispute or situation is being discussed by the Security Council);
- Giving recommendations for the peaceful settlement of any dispute which might harm the friendly relations among nations;
- Making recommendations on the powers and functions of any organ of the United Nations;
- Making recommendations to promote international cooperation, the development of international law, the protection of human rights, and international collaboration on economic, social, cultural, educational and health issues;
- Discussing reports from the Security Council and other UN organs;
- Approving the UN budget after deliberations;
- Electing the non-permanent members of the Security Council, the members of the Economic and Social Council (ECOSOC) and additional members of the Trusteeship Council (when necessary); to elect the judges of the International Court of Justice (jointly with the Security Council); and on the recommendation of the Security Council, to appoint the Secretary-General.
- Although the General Assembly's recommendations on global issues are considered an expression of world opinion, the Assembly cannot force a Member State to follow its recommendations on a particular issue.

The Assembly goes for its annual sessions from September to December. When required, a special session on subjects of particular concern may be called at the request of the Security Council, of a majority of the Member States, or of one member if the majority of the Member States agree. Moreover, an emergency session can be called within 24 hours in the same manner. An example of this was the Eleventh emergency special session of the United Nations General Assembly, which addressed the Russian invasion of Ukraine.

Each regular session of the General Assembly holds a General Debate at the beginning when many Heads of State come to express their views on critical international issues. Following the General Debate, most issues are discussed in one of the Assembly's six central committees:

First Committee (Disarmament and International Security);
Second Committee (Economic and Financial);
Third Committee (Social, Humanitarian and Cultural);
Fourth Committee (Special Political and Decolonization);
Fifth Committee (Administrative and Budgetary);
Sixth Committee (Legal).

Establishing and adopting the agenda is the first order of the day in each GA session. Most of the more than 160 items on the agenda are considered on a regular basis, and only a few new items are added or omitted each year. The recommendations by the six main committees and other such recommendations are adopted in plenary meetings in the form of resolutions and decisions, usually before the end of the regular session in December. Such resolutions and decisions are adopted by a majority of members present and voting. When it comes to taking decisions on important matters such as international peace and security, the election of members to other UN organs and budgets is decided by a two-thirds majority. The work that the United Nations does in the entire year is determined by the resolutions and decisions made during the Assembly's regular session. This work is carried out by various committees and other bodies established by the Assembly to study and report on specific issues, such as disarmament, peacekeeping, development and human rights.

Introduction to the Topic

Artificial Intelligence or AI is the biggest buzzword of recent times. The definition of an AI is as follows: Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. These machines can be trained to perform tasks that would usually require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. AI can be divided into two main categories: narrow or weak AI, designed specifically for some task, and general or strong AI, which can perform any intellectual task just like a human would do. Like all technology such as aeroplanes or rockets, AI was something seemingly out of a science-fiction novel. However, today we are surrounded by this artificial intelligence. Think of the voice assistants on your phone or the latest self-driving cars. AI is ubiquitous in our day-to-day life.

However, the rise of AI has opened up new vulnerabilities to national security and sovereignty. We can notice the use of AI in the realm of warfare, as in autonomous weaponry, cyberspace and cybersecurity among others. In the military domain, AI is enabling new autonomous capabilities and making them affordable to a wide range of actors. The dual use of AI has given weak states and non-state actors more prominence in warfare and options to enhance their capabilities. The use of AI in the cyber domain has led to the automation of various tasks which ranges from advanced persistent threat operations to intrusion detection and prevention systems designed for both offensive and defensive purposes.

The military potential of AI has brought path-breaking changes in the battlefields, with more autonomous systems coming into the security landscape. The interplay of this technology with the defence systems has enhanced asymmetric warfare options. There are diverse applications of AI in the military, including in the area of ISR; Military Logistics; CyberSpace Operations; Information Operations and Deep Fakes; Integrated Command and Control; Semi-Autonomous and Autonomous Systems; and LAWS. The effective use of AI in applications in rockets, missiles, aircraft carriers, and naval assets and its integration in C4I2SR has made it a critical part of the national security apparatus.

Artificial intelligence also opens up a plethora of legal issues such as liability. The emergence of AI and its significance has not eluded global superpowers. The US National Security Commission on Artificial Intelligence (NSCAI) described the potential of AI as "a source of enormous power for the companies and countries that harness them".

A rather peculiar and unique threat to security from the development of AI comes as a result of the intermingling of AI and social media. Bots who pretend to be humans, powered by AI are being used to influence social media which in turn can possibly influence the beliefs and opinions of the users. This can prove disastrous for state sovereignty.

History

The roots of Artificial Intelligence (AI) can be traced back to the 1950s when American computer scientist Alan Turing wrote an essay titled ‘Computing machinery and intelligence’. The term AI was then used as a title of a conference held at Dartmouth College in 1955. In this conference, which set in motion the future developments in the emerging field of Artificial Intelligence, John McCarthy (computer scientist), brought together top researchers from various fields for an open-ended discussion on Artificial Intelligence, the term which he coined at the very event. The definition of Artificial Intelligence is the ability of the computer system to perform tasks that normally require human intelligence. Automated machine learning and deep learning are significant areas of AI. AI also refers to the ability of machines to perform human-like cognitive tasks which include, thinking, perceiving, learning, problem-solving and decision-making as a constellation of technologies that enable machines to act with higher levels of intelligence.

During the Second World War, General George Patton won the D-Day campaign for the Allies without ever firing a shot. Patton was given charge of the First United States Army Group (FUSAG) and he led the FUSAG to fight a battle that did not involve arms and weapons but rather he used deception as a tool to convince the German command that the invasion point would be Pas de Calais rather than Normandy.

The FUSAG orchestrated a major force deployment—including hundreds of tanks and other vehicles—directly across the English Channel from it.

These tanks, however, were not what they seemed. The Allies used inflatable balloons painted to look like tanks to show the huge presence of the Allied forces. Although the strategy may sound like a technique employed by Jerry against Tom than George Patton against the German Nazis, it did the trick. German reconnaissance was fooled. The images captured by the Luftwaffe (aerial warfare branch of the German forces) planes were interpreted as a major buildup of forces in anticipation of an invasion of Pas de Calais, leaving the beaches of Normandy under-fortified.

Just as the FUSAG could expertly devise what patterns needed to be painted on the inflatable balloons to fool the Germans, with a type of AI attack called an "input attack," adversaries may craft changes in patterns of a target that will lead the AI system into making a mistake. When such inconsistencies are added in patterns in the target by an attacker which does not match with the variations in the dataset of the AI system, it may likely produce an arbitrary result. However, unlike the example of the inflated balloon tanks, these patterns or markings need not be as blatant. This is because AI algorithms process information differently than humans do. As a result, while it may have been necessary to make the balloons look like tanks to fool German officers who were relying on patterns, to fool an AI system, only a few stray marks or subtle changes to a handful of pixels in an image are needed to fail an AI system.

Apart from these input attacks, another type of AI attack—known as a poisoning attack—can fail an AI system from operating correctly in situations, or even insert a backdoor that can later be exploited by an adversary. Going by the same example, poisoning attacks would be the equivalent of hypnotising the German analysts to close their eyes anytime they were about to see any valuable information that could be used to hurt the Allies.

Current Situation

As a whole, these AI attacks have the characteristics of a severe cyber threat: they are versatile in form, widely applicable to many domains, and hard to detect. They may take the form of a smudge or squiggle on a physical target, or be hidden within the DNA of an AI system. They can target assets and systems in the real world, such as manipulating driverless cars to make "stop" sign invisible to them. In the cyber world, they may hide child pornography from content detectors seeking to stop its spread. AI attacks can be pernicious and difficult to detect which is a huge cause of concern. Attacks can be completely invisible to the human eye. Conversely, they can be grand and hidden in plain sight, camouflaging with their surroundings.

As AI is a disruptive technology, it is believed that it affects nearly all aspects of international security, from diplomacy, intelligence and defence, to conflict management. That's why more and more countries are growing interested in increasing their capabilities in artificial intelligence, in order to achieve dominance and collateral hegemony in international relations. AI could be the new weapon having the potential to cause mass destruction just like nuclear power. It may rewire the global order, and all countries could seek to have it with its dual usage, civilian and military.

AI security risks are not confined to theoretical analyses but also to AI deployments. For instance, attackers can craft files to bypass AI-based detection tools or add noise to smart home voice control commands to invoke malicious applications. Attackers can also tamper with data returned by a terminal or deliberately engage in malicious dialogues with a chat robot to cause a prediction error in the backend AI system. Applying small stickers on traffic signs or vehicles can lead to false inferences by self-driving vehicles. To mitigate these AI security risks, AI system design must find a way to deal with the following five security challenges:

- Software and hardware security: The models, platforms, code of applications and chips may have vulnerabilities or backdoors that attackers may identify and exploit. Further, they may create backdoors in models to launch advanced attacks. Due to complications in the AI models, it is difficult to identify backdoors.

- Data integrity: Attackers can install malicious data in the training stage to affect the inference capability of AI models or add a small perturbation to input samples in the inference stage to cause changes in the inference result.

- Model confidentiality: Service providers generally want to provide only query services without exposing the training models. However, an attacker may create a clone model through several queries.

- Model robustness: AI training samples typically do not cover all likely situations, resulting in the insufficiency of robustness. Therefore the model may fail to provide correct inference when it comes to out-of-the-ordinary situations.

- Data privacy: In situations where AI systems learn by the training data provided by users, attackers can repeatedly query such a trained model to obtain users' private information.

In other words, AI is trying to scrape through the systems, networks, databases, and human behaviours to find any minutest deviations or anomalies that increase the possibility of cyber threats. It gives an indication of not only what could be used to attack systems but also what is most likely to be used to attack the systems.
The future would be shaped by AI-enabled technologies, but they cannot determine it completely. It is up to nations, groups, and individuals how they employ and respond to the various uses of AI. The policies that nations may adopt can guide, restrict, or encourage certain uses of AI. To manage the challenges of the future, every country must adopt a national strategy on how to eke out benefits from AI, but at the same time mitigate its disruptive effects.

AI applications in the physical world--suppose in the transportation sector--brings into focus the question of human safety, and the need to create systems that can competently react to unforeseen situations, and have minimum unintended consequences. AI also has implications in the cybersecurity domain. On the one hand, AI systems may be associated with causing cyber security risks, and on the other, AI can be applied to counter cybersecurity vulnerabilities, from spam filtering to detecting serious cybersecurity risks and addressing cyber threats.

AI is now being considered the driving horse of foreign relations and global security. Technology entrepreneur and founder of OpenAI (the company that created ChatGPT) Elon Musk and noted physicist Stephen Hawking have predicted the danger of AI and the end of the human race as a consequence of developments in AI. Despite that, such developments in the field of AI have continued which have put new topics on the international agenda, challenged geostrategic relations, served as a tool for diplomats and negotiators, and created new opportunities and concerns about human rights. Diplomacy is homogenous to a strategic board game involoving multiple opponents. Every nation aspires to win and takes steps according to the moves and progress of other nations. AI is considered top-notch at board games. For instance, AI has defeated Chess grandmasters in a go. One such example is the AI powered IBM supercomputer Deep Blue which defeated Chess grandmaster Garry Kasparov in 1997. In 2019, an AI program developed by Carnegie Mellon University in association with Facebook AI called Pluribus, defeated the leading professionals in Texas hold ’em poker which is considered to be the most popular form of poker in the world. The development of AI technology is central to the economical aspect, which can reshuffle losers and winners.

International Laws and Legislations; Convention on Certain Conventional Weapons

The biggest challenge with Artificial Intelligence is regulation. Whenever there is a discussion on LAWS (Lethal Autonomous Weapons Systems) and AWS (Autonomous Weapon Systems), the most common solution is to point towards the CCW or the Convention on Certain Conventional Weapons. The Convention on Certain Conventional Weapons (CCW) is an international treaty that regulates the use of certain weapons that are considered to cause unnecessary or unjustifiable suffering to combatants or affect the civilian population. The CCW bans or restricts the use of landmines, incendiary weapons, and booby-traps, as well as weapons that blind or otherwise incapacitate their victims. The CCW also regulates the transfer and stockpiling of these weapons. The convention was adopted in 1980 and has been ratified by over 110 countries.

On the issue of LAWS, the Group of Governmental Experts came up with the following 11 guiding principles in 2019:
(a) International humanitarian law would continue to apply fully to all weapons systems, which includes the potential development and use of lethal autonomous weapons systems;
(b) Since accountability cannot be transferred to machines, humans must retain responsibility for decisions on the use of weapons systems. This should be considered across the entire life cycle of the weapons system;
(c) Interactions between humans and machines, which may take various forms and be implemented at various stages of the life cycle of a weapon, should ensure that the potential use of weapons systems based on emerging technologies in the area of lethal autonomous weapons systems is in accordance with applicable international law, particularly the International Humanitarian Law. In determining the quality and extent of human-machine interaction, several factors should be considered including the operational context and the characteristics and capabilities of the weapons system as a whole;
(d) Accountability for developing, deploying and using any emerging weapons system in the framework of the CCW must be ensured as per the applicable international law, including through the operation of such systems within a responsible chain of human command and control;

(e) In accordance with States' obligations under international law, in the study, development, acquisition, or adoption of a new weapon, means or method of warfare, it must be determined whether its employment would, in some or all circumstances, be prohibited by international law;
(f) While developing or acquiring new weapons systems based on emerging technologies in the area of lethal autonomous weapons systems, physical security, appropriate non-physical safeguards (including cyber-security against hacking or spoofing of data), the risk of proliferation and or acquisition by terrorist groups should be considered;
(g) Proper risk assessments and mitigation measures should be part of the design, development, testing and deployment cycle of emerging technologies in any weapons systems;
(h) Consideration should be given to the application of emerging technologies in the area of lethal autonomous weapons systems in upholding compliance with International Humanitarian Law and other applicable international legal obligations;
(i) In crafting potential policy measures, emerging technologies in the area of lethal autonomous weapons systems should not be anthropomorphized, in other words they should not be given human-like attributes;
(j) Discussions, deliberations and any potential policy measures taken within the context of the CCW should not hinder progress in or access to peaceful and productive uses of intelligent autonomous technologies;
(k) The CCW offers an appropriate framework to deal with the issue of emerging technologies in the area of lethal autonomous weapons systems within the context of the objectives and purposes of the Convention, which seeks to strike a balance between humanitarian considerations and military necessity.

The CCW tried to debate and resolve the issue of LAWS through discussions in 2021. The talks ultimately adjourned without a consensus on the “Killer robots”.

Key Issues

Mentioned below are some of the few key issues/debates surrounding the topic of AI and Security ;

- What is the position of AWS and LAWS in IHL and ICL?
- What are the ethics surrounding the use of AWS and LAWS and how can they be regulated?
- How has the use of AI impacted Cyber Security at large, and what are some new areas of vulnerabilities and how can they be rectified?
- How can we deal with the dual-nature of AI ?
- What can be done about non-state actors accessing Artificial Intelligence?

Bloc Positions

Governments around the world have developed AI frameworks and policies to help prompt economic and technological growth. The frameworks range from India's National Strategy for AI #AIforAll, the US executive order on AI leadership, China's Next Generation Artificial Intelligence Development Plan" to "AI Made in Germany" and the "Pan-Canadian AI Strategy, among others. These strategies primarily focus on talent and education, research and development, investment by the government and collaborations with other nations and regulatory frameworks for the best development and progress and the deployment of AI.

United States of America: In 2019, the then President of United States Donald Trump emphasized the significance of ensuring American leadership in the development of emerging technologies, including AI, that makes up the Industries of the Future. At the same time, Donald Trump had signed an Executive Order to launch the American AI Initiative with the objective of stimulating US's national leadership in AI. The American AI initiative includes five key areas of emphasis: Investing in AI Research & Developement; Setting AI Governance Standards; Building the AI Workforce; Unleashing AI Resources; and International Engagement and Protecting America's AI Advantage.

China: China had announced the Next-Generation Artificial Intelligence Development Plan in 2017. The Plan includes initiatives and goals for industrialization, talent development, Research & Development, education and skills acquisition, standard-setting and regulations, ethical norms, and security. The country has also a national AI strategy and has announced its plan to invest tens of billions of dollars in AI research and development.

Singapore: In May 2017, Singapore launched a five-year national program called AI Singapore worth 150 million Singapore Dollars, to enhance the country's capabilities in AI. In June 2018, the Singapore government also announced three new initiatives on AI governance and ethics.

France: In 2017, France launched its national AI strategy, “AI for Humanity”, which was developed by French mathematician Cédric Villani to turn France into an AI leader. A year later, President Emmanuel Macron divulged a €1.5 billion plan to make the country a global leader in AI research and innovation at the end of the AI for Humanity Summit in Paris. The plan details how to align France’s resources around talent, and open data ecosystem, research institutions, and the ability to address ethical issues and enhance specific sectors of the country’s economy.

United Kingdom: In April 2018, the UK government issued its national AI strategy, “AI Sector Deal” with the objective of creating an economy that harnesses artificial intelligence. It includes policies to strengthen public and private Research & Development, investment in STEM education, enhancement of digital infrastructure, promoting AI talent, and leading the global conversation on data ethics.

Canada: Canada is the first country in the world that introduced a 25 million Canadian Dollar national AI strategy known as the Pan-Canadian Artificial Intelligence Strategy, in 2017. The strategy has four goals and objectives: establish three clusters of scientific excellence, develop thought leadership on the economic, ethical, policy, and legal implications of AI, increase the number of AI researchers and graduates and support the national research community on AI.

Germany: In November 2018, Germany released its AI Strategy, “AI Made in Germany”. A year later, in the 2019 federal budget, the country allocated a total of €500 million to reinforce the AI strategy for 2019 and the following years. Germany aims to provide around €3 billion over the next seven years starting from 2018 for the implementation of the Strategy.

United Arab Emirates: In October 2017, the UAE Government launched its AI strategy called the “UAE Strategy for Artificial Intelligence (AI)”. The strategy aspires to: achieve the objectives of UAE Centennial 2071; boost government performance at all levels; use an integrated smart digital system that can overcome challenges and provide efficient and effective solutions; make the country the first in the field of AI investments in various sectors; and create a new vital market with high economic value.

India: In June 2018, the country released its AI strategy, “National Strategy for Artificial Intelligence #AIforAll.” NITI Aayog, the think tank of Indian government has identified five focus areas where AI development could enable both growth and greater inclusion. These include agriculture, healthcare, education, urban-/smart-city infrastructure, and transportation and mobility. NITI Aayog also provides over 30 policy recommendations to promote re-skilling and training, invest in scientific research, expedite the adoption of AI across the value chain, and reinforce ethics, privacy, and security in AI.

Japan: In 2016, the then Japanese Prime Minister Shinzō Abe called for the Japanese government to establish an “Artificial Intelligence Technology Strategy Council”, which formulated the “Artificial Intelligence Technology Strategy” in March 2017. In July 2017, the country published the “Draft AI R&D GUIDELINES for International Discussions” in preparation for “the Conference toward AI Network Society”. In November 2017, an AI-powered bot “boy” named Shibuya Mirai was granted residency in Tokyo, Japan. Moreover, in June 2018, the Japanese government announced that AI would also become an official part of its “integrated innovation strategy.”

Bibliography

- https://www.iss.europa.eu/content/artificial-intelligence-%E2%80%93-what-implications-eu-security-and-defence

- https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/

- https://www.oecd-ilibrary.org/sites/cc3a9728-en/index.html?itemId=/content/component/cc3a9728-en

- https://www.diplomacy.edu/topics/ai-and-diplomacy/#:~:text=Greater%20scrutiny%20is%20necessary%20because,concerns%20about%20protecting%20human%20rights

- https://www.idsa.in/issuebrief/ai-and-national-security-ssharma-120922#:~:text=The%20use%20of%20AI%20in,both%20 offensive%20and%20 defensive%20 purposes.