VTMUNC

est. 2024

# Disarmament and International Security Committee General Assembly Committee

# Table of Contents

*For Each Topic:*

# Letter From the Secretariat

**Dear Delegates of VTMUNC II,**
We appreciate your participation and dedication to the premier Virginia Tech Model United Nations Conference's efforts to promote productive and civil discourse and conversation. Nevertheless, please be warned that some presentations, discussions, and or information found in the background guides may contain delicate or triggering material. At Virginia Tech, we prioritize fostering a safe and inclusive environment, so we want to ensure that you are prepared for the nature of the discussions to occur.
That being said, the following content areas may contain sensitive material:

1. **Conflict Zones & Human Rights Violations**: Some conversations may involve sensitive global problems including human rights violations, armed conflicts, and or other difficult themes.
2. **Sensitive Cultural or Religious Topics:** Some topics may raise sensitive cultural or religious issues for individuals.
3. **Violence and Trauma:** In their speeches or resolutions, delegates may reference incidents of violence, trauma, or abuse in real-world scenarios that may potentially be a sensitive topic to delegates in committee.
4. **Discussions about Discrimination and Marginalization:** Emotionally intense discussions concerning discrimination, marginalization, or inequity may arise during committee.

As you prepare for the conference, we encourage all of our delegates to approach these discussions with both respect and empathy for differing perspectives. If the content of these committees is something that you are uncomfortable with, we recommend that you take the appropriate steps to prioritize your well-being, such as seeking support from conference staff or Secretariat of VTMUNC II. Bound by the motto Ut Prosim (That I May Serve), we serve to ensure that we will promote constructive and respectful dialogue during committee sessions. As you prepare and participate in the conference, we promise that VTMUNC II will stay committed to creating a space where all your voices are heard and are welcome. Thank you for your compassion and cooperation to our goal of respectful and intellectual discourse for all. We hope that as you progress with our conference, you continue to bloom.

**Sincerely,**
**Shriya Chemudupati, Secretary General of VTMUNC II**
**Anneli Sample, Under-Secretary General of General Assemblies of VTMUNC II**
**Holly Johnson, Under-Secretary General of Crisis Committees of VTMUNC II**
**Thomas Quinn, Under-Secretary General of Specialized Agencies of VTMUNC II**

# Conference Guidelines

The first iteration of the Virginia Tech Model United Nations Conference, otherwise known as VTMUNC II, is committed to providing a safe and pleasurable experience for all delegates, advisors, and individuals involved with VTMUNC II. Although participating in Model UN is being involved in competitive activity, its fundamental purpose is to uphold and put into practice both the principles of diplomacy, collaboration, and cooperation. Any individual that violates the policies and procedures of VTMUNC II and the ideals of an open and inclusive environment will be subject to disciplinary action from the staff of VTMUNC II; disciplinary action may include a warning or being disqualified from receiving awards. Promoting an environment that is open to all by being safe, equitable, and exhilarating is our utmost priority. In order to ensure this, the following are prohibited:

1. Any pre-writing or working on committee content outside of VTMUNC II committee sessions (as described by the Schedule of Program).
2. Any speeches, directives, crisis arcs, or actions in committee that intend to create violence or promote a violent environment to a specific group of people, including mentions of sexual violence, graphic violence, and other behavior that is beyond committee guidelines.
3. Any hate speech, written documents, or behavior that uses language that is discriminatory and disrespectful, including but not limited to any language that is racist, sexist, homophobic, transphobic, xenophobic, antisemitic, Islamophobic, or language harmful to any specific group.
4. Any actions that are deliberate, both knowingly and intentionally, to bully, harass, or otherwise harmful behavior that may or has hurt other delegates' physical and or mental health.

# Overview of General Assembly Committees

Much like the real United Nations, Congress, Parliament, and other legislative bodies, the General Assembly follows basic parliamentary procedure to promote collaboration between states, share ideas to everyone in the room, and create the most effective solutions to the world's most pressing issues. Delegates will debate what the agenda should be set to, discuss the chosen topic in depth, and write and debate solutions.

General Assembly committees are largely comprised of two types of caucuses, described below:

Moderated Caucuses: One state at a time gets the floor for a specified amount of time and directly addresses fellow delegates and the chair about a specified topic voted on by the delegates. This time is used to share ideas, argue for or against something, and move the committee in the direction the delegate wants it to go.

Unmoderated Caucuses: Delegates may move freely throughout the room and speak with each other to share ideas, form blocs, and write working papers. In double delegation committees, one delegate may stay in the room to participate in a simultaneous moderated caucus while the other leaves the room to discuss with their bloc, if the chair allows it.

# Letter From the Chair

Hey everyone!

My name is Sarah Sass and I will be your head chair for this GA committee! I am a junior chemical engineering major with a minor in green engineering from Norfolk VA, and I've been doing Model UN since high school. I started in sophomore year of high school, founding my club with my friends, and now I am co-vice president of our MUN@VT club here at tech! Outside of MUN, I do research on carbon capture in the Chemistry department and I like to spend my time reading or being with my friends. At VTMUNC I, I ran a crisis committee about Harry Potter, and it was a ton of fun seeing the crazy things people did. I am super excited to be running a general assembly committee this year, as when we compete on the collegiate level, I am typically in these types of committees. Working together diplomatically and finding unique solutions for real world problems is my favorite part of Model UN, and I'm looking forward to seeing what you guys will do. Let me know if you guys have any questions or concerns about this committee! See y'all in February!

Sarah Sass
DISEC Head Chair

# Topic A: Cyber-Security and AI
# Background

Artificial intelligence, or AI, is revolutionizing the way we approach cybersecurity, transforming it from a method of defense to a preventative. The advent of AI in cybersecurity has been used to train machines to detect malware threats enabling a proactive approach to "threat hunting" ("What Is AI in Cybersecurity?"). Cybersecurity refers to the measures taken to protect computer systems, network, and data from theft, damage, or unauthorized access. However, the duality of AI remains in its ability to be both the shield and the sword – enhancing defense by automating threat detection, but also raising new risks that can be exploited by hacktivists.

Unlike traditional methods, AI can sift through and process vast amounts of data, detect patterns, and adapt to evolving threats– much faster than humans can. For example, AI utilizes machine learning, neural networks, and other techniques to analyze network traffic and identify potential breaches and detect patterns that could indicate potential threats to a system's security. However, the same technology can be weaponized (SentinelOne). Hackers often use AI to automate their attacks, create convincing deep fake videos, or exploit vulnerabilities in systems at an unprecedented rate. They can also utilize AI to bypass malware detection by training the software to bypass traditional security measures ("How Hackers and Scammers Use AI (Artificial Intelligence)").

There have been many real-world examples of incidents, such as the SolarWinds attack, where advanced automation techniques were used to compromise thousands of systems globally. During this attack SolarWinds' software supply chain was breached, allowing attackers to gain access into the networks of prominent organizations, including U.S government agencies, such as the Homeland Security, State, Commerce, and Treasury. The attack remained undetected for months, displaying the weaknesses and vulnerabilities of supply chain software and the sophistication of modern cyber threats (Oladimeji). This example illustrates how AI-powered cyberattacks could destabilize governments, disrupt economies, and harm individuals. Moreover, the absence of universal regulations on AI's use in cybersecurity leaves nations and corporations vulnerable to exploitation and abuse.

# Current Situation

As explained within the background, Artificial intelligence has developed exponentially in the last decade. In response to this, many businesses have begun to harness this tool to utilize it for many fields, including data analysis, generating content, optimizing IT functions, and cybersecurity (Quiroz). Within this increase in use in AI for commercial and private means, concerns on the safety and security of this technology have grown globally. Many countries have begun discussions on passing laws or regulations on AI technology, as it can pose a risk for national security. Though there is a push for individual countries to protect themselves and their citizens against the risk this new technology has posed to cybersecurity and cybercrime, there has yet to be a true united global response that standardizes regulations and includes every country in the conversation.

Countries like the United States have established several sector-specific AI-related agencies and organizations that address some of the challenges arising, but have left much of the regulation up to the states themselves. The European Union has taken a more combined approach, with measures like the General Data Protection Regulation (GDPR) and debates on the planned Artificial Intelligence Act (Jacob). These initiatives aim to set strict guidelines for gathering, using, and preserving personal information. The EU's motivation is largely based on individual privacy and ensuring data protection for its citizens, giving most of the regulatory jurisdiction to itself. It also stands to promote transparency to ensure accountability on all ends. In China, they have also adopted cybersecurity and AI related regulations, including the Chinese Cybersecurity Law and the New Generation AI Development Plan, that provide measures for data protection, emphasizing compliance and timely risk management. China has become a global leader in AI development overall, so many of their regulations also emphasize development of these technologies (Jacob).

As it stands now, the growth of Artificial Intelligence technologies is not slowing down, and with it the risk of cybersecurity threats will continue to increase. Without proper regulation from the global community as a whole, there will be irreversible damage to data security and protection. Countries and member states need to band together to strike the right balance between investing within the development of AI and protecting individuals' data from the technology itself.

## Past Actions

While countries have taken regulatory steps to address the challenges that arise with the advent of AI technology, the United Nations itself has taken several measures to further balance the matter. The UN Global Programme on Cybercrime, a segment of the UN Office on Drugs and Crime, emphasizes the need for cooperation between countries, as well as an overall increase in institutional and individual skill to effectively combat cyber attacks. This sector also aims to increase population awareness and knowledge on cybercrime to reduce the risks of one being susceptible to cyber attacks ("Global Programme on Cybercrime"). Additionally, the International Telecommunication Union, ITU, performs a similar task, with the goal to "protect and support everyone's fundamental right to communicate" (United Nations) Furthermore, the ITU takes upon itself projects, such as "Cyber for Good," which aim to bridge the gap in cybersecurity knowledge between larger, more developed countries, and the LDR, Least Developed Countries ("Cyber for Good")

However, these overall initiatives have yielded mixed results. On one hand, national regulations like the GDPR passed new policies to enhance data protection, establish legal frameworks, and increase transparency. On the other hand, countries have failed to create a unified framework for AI regulation, let alone a unified response to AI utilization in cyber security (Park). This fragmented approach has left gaps in global cybersecurity defenses, making it difficult to address the rapidly growing threats posed by AI. Until a comprehensive, coordinated global strategy is implemented, the effectiveness of these efforts will remain limited, and the risks associated with AI will continue to grow.

## Questions to Consider

1. How can countries and member states within the United Nations tackle this issue together while avoiding infringing on national sovereignty and the rights of the companies around the world that own many of the emerging AI technologies?
2. Does advancing AI research and development inherently lead to more of a risk for global cybersecurity, or does it do the opposite by allowing more information about these technologies to be circulated?
3. What does your country stand to lose or gain with more regulation on AI tech specifically in regards to national security?

## Bibliography

"How Hackers and Scammers Use AI (Artificial Intelligence)." *Cyber-Seniors*, https://cyberseniors.org/uncategorized/how-hackers-and-scammers-use-ai-artificial-intelligence/. Accessed 19 November 2024.

Jacob, Savio. "AI Regulations Around the World: A Comprehensive Guide To Governing Artificial Intelligence." *Spiceworks*, 30 April 2024, https://www.spiceworks.com/tech/artificial-intelligence/articles/ai-regulations-around-the-world/. Accessed 10 January 2025.

Oladimeji, Saheed. "SolarWinds hack explained: Everything you need to know." *TechTarget*, 3 November 2023, https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know. Accessed 10 January 2025.

Quiroz, Camilo. “What is Artificial Intelligence (AI) in Business?” *IBM*, https://www.ibm.com/think/topics/artificial-intelligence-business. Accessed 10 January 2025.

SentinelOne. “What is Artificial Intelligence (AI) in Cybersecurity?” *SentinelOne*, 10th May 2024, https://www.sentinelone.com/cybersecurity-101/data-and-ai/artificial-intelligence-in-cybersecurity/#:~:text=AI%20in%20cybersecurity%20refers%20to,cybercrime%20and%20ensure%20cybersecurity%20proactively. Accessed 19th November 2024.

“What Is AI in Cybersecurity?” *Sophos*, https://www.sophos.com/en-us/cybersecurity-explained/ai-in-cybersecurity. Accessed 19 November 2024.

“Global Programme on Cybercrime” United Nations : Office on Drugs and Crime, www.unodc.org/unodc/en/cybercrime/home.html.

United Nations. “Telecommunication Union | United Nations.” United Nations, www.un.org/en/academic-impact/itu#:~:text=The%20International%20Telecommunication%20Union%20is,everyone's%20fundamental%20right%20to%20communicate.

“Cyber for Good.” ITU, www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyber4Good/Cyber4Good.aspx#:~:text=WHAT%20CYBER%20FOR%20GOOD%20IS,supporting%20developing%20countries'%20cybersecurity%20improvement.

Park, Sangchul. “Bridging the Global Divide in AI Regulation: A Proposal for a Contextual, Coherent, and Commensurable Framework.” SSRN Electronic Journal, Jan. 2024, https://doi.org/10.2139/ssrn.4950781.

# Topic B: Space Travel and Surveillance Background

Historically, the space race during the Cold War between the U.S. and the Soviet Union shaped space exploration. The Space Race began with the launch of the Soviet Union's Sputnik 1 in 1957, the first artificial satellite. In fierce competition, the U.S. established NASA (National Aeronautics and Space Administration) in 1958. In response to the Sputnik 1, NASA began their Apollo missions, through which the Apollo 11 mission in 1969, the United States was able to land humans on the moon. Despite the Cold War rivalry, some aspects of space exploration became cooperative. One of the most important examples is the Apollo-Soyuz Test Project in 1972, where U.S. and Soviet spacecraft docked in space. This was the first spaceflight collaboration. Later, the International Space Station became the primary example of international cooperation in space. The International Space Station involves many nations' space agencies working together including the U.S., Japan, Russia, and the European Space Agency, along with private companies.

Space exploration is complicated and expensive, both of which require countless resources. No one country can afford to fund space exploration projects without the support from other nations. Cooperation allows nations to pool their resources and share finances. For example, the International Space Station is a prime example of how sharing resources and expertise can lead to great advancements in space exploration. Additionally, history has shown that international collaboration in space can help maintain diplomatic relationships among nations. In the past, the International Space Station is how enemies during the Cold War found common ground. At the same time, there are so many reasons why nations do not share their knowledge or lend a helping hand. Countries with advanced space programs can project power and technological leadership. Space is also strategically important for national security, as space-based surveillance and communication systems are essential to national defense. Why would a nation want to jeopardize their possible prestige and power at risk. Not only this, but some argue that competition drives technological innovation. Healthy competition pushes technological boundaries and achieves goals faster than if nations were to collaborate. Finally, as for geopolitical competition, nations are already positioning themselves to lead the way as topics of colonization and Mars exploration arise. If one nation gains a major advantage in space, there are chances it could shift the balance of power on Earth.

# Current Situation

Hacking is becoming more and more common. With the possibility of breaches, sensitive data in a space based surface is at risk. Not only this, but cyber-attackers have also taken full control of nations' communication links. In the 2008 Russian Cyberattack on U.S. satellites, the Russians targeted the U.S. Air Force's military satellites. This incident highlights the vulnerability of security in the world of space. While cybersecurity attacks are an extremely important concern, privacy concerns impact each and every one of us. The government secures a vast majority of their personal and environmental data from satellites, but then questions arise of who has and uses the data. The ethical concerns surrounding this topic are the misuse and overreach of data as well as the lack of transparency in data-sharing agreements. We are always being watched and tracked without our consent. What happens when our information is compromised? Additionally, with the increase of AI in the satellite systems, questions regarding autonomous decision-making arise. AI-powered surveillance identifies and tracks targets without the need for human oversight. Who then is held accountable for the risk of biased decisions made. It is imperative that there are new guidelines set surrounding space-based surveillance.

# Past Actions

In 1967, more than 100 countries signed a treaty called "The Outer Space Treaty" which set guidelines and rules for space exploration. Some of these guidelines included no nation should be using space as a military benefit and all nations should be of help in need of emergency landings for astronauts. This treaty was extremely important because it is what maintained international peace and cooperation among nations. Moreover, this treaty also ensured to hold nations accountable for their actions in case any laws were broken or damages were caused. While this was the key to positive change in the past, this treaty is becoming less relevant each year due to the increase in private sectors involved in space as well as an increase in space militarization like never before. It may be time to reconsider and come up with new possible regulations.

The UN as a whole promotes a cooperative view to space travel and exploration, believing that all should be able to access and benefit from space as a whole (United Nations). The United Nations currently has five different treaties that do a multitude of things. An example, as discussed earlier, is the Outer Space Treaty. All of these agreements aim to promote and protect peace in regards to outer space, and hope to settle disputes fairly when they arise. Peaceful cooperation is also promoted through the United Nations Office for Outer Space Affairs (UNOOSA), a permanent UN committee that works to establish or strengthen the legal and regulatory frameworks for space activities, and assists developing countries in using space science and technology for sustainable socio economic development (“United Nations Office for Outer Space Affairs”).

## Questions to Consider

1. Today, so many countries are seeking to explore the Moon, Mars, and beyond, should these countries be allowed to pursue their own interests, even if it is at the expense of international cooperation?
2. What role does space exploration play in the future as a whole? What can be gained from advancing into the new frontier and how can that benefit or hurt a country?
3. With many changes in technology since the original space race, space exploration looks a lot different. How do these new technologies help or hurt the push for space travel?

## Bibliography

United Nations. “Global Issues: Outer Space.” *United Nations*, https://www.un.org/en/global-issues/outer-space#:~:text=All%20humankind%20should%20benefit%20from%20the%20exploration%20of%20space&text=Outer%20space%20shall%20be%20free,or%20by%20any%20other%20means. Accessed 10th January 2025.

“United Nations Office for Outer Space Affairs.” *Wikipedia*, https://en.wikipedia.org/wiki/United_Nations_Office_for_Outer_Space_Affairs. Accessed 10 January 2025.

"The Space Race: A Timeline of the U.S. vs. Soviet Union Space Exploration Competition." *NASA*, NASA, 12 Apr. 2021, www.nasa.gov/feature/the-space-race-a-timeline-of-the-u-s-vs-soviet-union-space-exploration-competition

"The 2008 Russian Cyberattack on U.S. Satellites." *The New York Times*, The New York Times Company, 13 Oct. 2020, www.nytimes.com/2020/10/13/technology/russia-cyberattack-us-satellites.html.

"Outer Space Treaty." *United Nations Office for Outer Space Affairs*, United Nations, 2021, www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.

"International Space Station." *NASA*, NASA, 3 Nov. 2023, www.nasa.gov/mission_pages/station/main/index.html.