

# **UNGA**

## **BACKGROUND GUIDE**



### **Agenda**

**“Addressing the Global Rise in  
Cyberbullying and Online Harassment.”**

## **LETTER FROM THE EXECUTIVE BOARD**

We are pleased to preside over this year's United Nations General Assembly session at JAMUN 2025.

The committee will focus on the agenda: “Addressing the Global Rise in Cyberbullying and Online Harassment.”

The significance of this agenda is immense, as these digital challenges affect international security, personal well-being, and the integrity of societies. Your role as delegates is not simply to participate in debate, but to meaningfully engage with issues that have a real impact on the lives of people worldwide.

We anticipate that many of you may have questions about what is expected. You are invited to ask any of us, and we will gladly help you. Above all, we ask you to approach this committee with seriousness and respect for the importance of the topic. Let your research and discussions be rigorous and insightful; every contribution should reflect the gravity of cyberbullying and online harassment. Remember, these are not distant problems but immediate realities faced by nations and individuals.

Consider the influence that technology, social media, and policy can have on this agenda, and use your platform to explore both the challenges and solutions. The background guide is designed to give you a strong foundation, but genuine excellence comes from pursuing deeper research, considering a range of perspectives, and offering creative, well-supported solutions. Independent exploration will enhance not only your own understanding, but also the quality of committee debate.

We encourage you to critically assess evidence, challenge assumptions, and engage with the agenda passionately and constructively. We look forward to the energy you will bring and the thoughtful dialogues that will shape our work together.

Good luck with your preparations — we eagerly anticipate your presence at JAMUN 2025 and the valuable debates to come. For any queries, feel free to contact the Executive Board!

Warm regards,

***The Executive Board***

Shrey Naithani  
[snaithani1212@gmail.com](mailto:snaithani1212@gmail.com)  
+91 8383052633  
Chairperson

Aarav Rajpal  
[aaravrajpal21@gmail.com](mailto:aaravrajpal21@gmail.com)  
+91 8595289154  
Vice Chairperson

Agreema Kapoor  
[agreemakapoor@gmail.com](mailto:agreemakapoor@gmail.com)  
+91 8076572474  
Vice Chairperson

Aarna Gupta  
[aarnagupta31@gmail.com](mailto:aarnagupta31@gmail.com)  
+91 8448249465  
Rapporteur

Prakshaal Jain  
[prakshaaljain77@gmail.com](mailto:prakshaaljain77@gmail.com)  
+91 9911212143  
Rapporteur



# **COMMITTEE INTRODUCTION**

The United Nations General Assembly (UNGA) is one of the six main bodies of the United Nations (UN) and acts as its primary forum for discussion, policymaking, and representation. Its structure, authority, and procedures are defined in Chapter IV of the UN Charter.

The UNGA oversees the UN's budget, elects non-permanent members to the Security Council, appoints the UN secretary-general, reviews reports from other UN organs, and issues recommendations through resolutions. It also creates various subsidiary bodies to support its wide-ranging objectives. The General Assembly is the only UN body in which every member state enjoys equal representation.

Meetings of the General Assembly are held annually at the UN Headquarters in New York City, presided over by its elected president or the UN secretary-general.

The UNGA has six Standing Committees, which all discuss Specific topics:

- I. Disarmament and Security
- II. Economic and Financial
- III. Social, Humanitarian and Cultural
- IV. Special Political and Decolonisation
- V. Administrative and Budgetary
- VI. Legal

The General Assembly has been passing several resolutions since its foundation in 1946. It helps by acting as a forum for multilateral discussion on international issues, setting standards, and making recommendations on global challenges, including peace, security, and sustainable development.

The General Assembly In the Model United Nations:

This committee in JAMUN aims to mimic reality by reproducing the stages of foreign policies and decision making, with delegates representing nations from all across the globe.

## **Basic Guide to Research**

Research should not be mere copy-pasting of information you find, but understanding it, analysing it from the perspective of your country and thinking of what else can be done regarding the problem in hand.

Here are a few steps you can follow.

### **1. Know your committee**

When researching, make sure to take time to learn how your specific UN committee works. It is a suggestion to find answers to the following questions:

- What does your specific body do? (Does it send troops? Disarm? Help children? World hunger? Alternative energy?)
- What is its history / major past actions it has done? This is important because it tells you what is allowed/encouraged.
- Is what you're offering new or an extension/improvement of what was?
- What is it doing now?
- What are its limitations?

### **2. Analyse your country**

To represent your allotted nation effectively, you must have a solid understanding of:

- Polity and government structure
- Economy and trade policies
- Military capabilities and security concerns
- Allies and opponents
- Location and neighbours
- Main language
- Major industries and famous things
- Recent news events
- How is your country and its people affected?
- Stance on global issues

A well-rounded understanding of these areas ensures that your representation is realistic and grounded.

### **3. Study Your Country's Foreign Policy**

Foreign policy reflects how a nation interacts with others politically, economically, socially, and militarily, always with the goal of protecting its national interest.

How to analyze foreign policy:

Identify your country's official stance on the agenda and related subtopics.

alliances and disagreements may vary depending on the matter.

Example: India may strongly disagree with Pakistan on terrorism and Kashmir, but still maintains a positive outlook on trade.

#### **4. Research the Agenda Thoroughly**

Start with the Background Guide to gain an overview. While researching, look at the agenda through all its aspects, including the social, health, environmental, economic, educational, and political impacts of the topic.

You also need to know what global (international organizations, unions, committees etc.) and national policies have already been implemented. You need to know what was done before to know what to do next.

Solution part of your research should include what loopholes exist in existing legal frameworks, how to address them, and what your country can propose at a world forum like the UN according to your country's stance.

#### **Final Note**

Research is the foundation of strong diplomacy. Your preparation should combine depth, credibility, and clarity. By the end of your research you should be able to answer these questions about your agenda according to its relevance-

- What?
- Why?
- How?
- Where?
- When?
- What is expected if no one intervenes?

This background guide gives you a structure to work with, your research in no way should be limited to it.

Happy researching!!

## **Proofs and evidence accepted in the committee**

Evidence or proof will be accepted as credible in the committee from the following

1. **Reuters**– It is one of the world's most trusted providers of answers. It is an independent private news agency, which mostly covers international events of importance. (<http://www.reuters.com/> )

2. **State operated News Agencies**– These reports can be used in the support of or against the State that owns the News Agency. These reports, if credible or substantial enough, can be used in support of or against any country as such but in that situation, they can be denied by any other country in the council.

For example-

a. RIA Novosti (Russia) <http://en.rian.ru/>

b. IRNA (Iran) <http://www.irna.ir/ENIndex.htm>c. Xinhua News Agency and CCTV (P.R. China) <http://cctvnews.cntv.cn/>

3. **Government Reports: The EB recognises news from government reports as credible.**

a. Government Websites like the State Department of the United States of America (<http://www.state.gov/index.htm>)

b. Ministry of Foreign Affairs of various nations like India (<http://www.mea.gov.in/> ) People's Republic of China (<http://www.fmprc.gov.cn/eng/> )

4. **Permanent Representatives to the United Nations**

The documents from individual country websites also serve as a source for finding official statements by that country on various agendas. The nature of websites vary a lot from country to country.

[www.un.org/en/members/](http://www.un.org/en/members/)

## 5. Other Multilateral or Inter-Governmental Organisations

These are international organisations which are not a part of the United Nations. Usually one

may find these organisations based around a specific region like South Asia, and with a specific purpose such as trade, security or cooperation. Documents from the same can be deemed credible, most certainly for the countries which are a part of that organisation.

For example

a. South Asian Association for Regional Cooperation (SAARC)

Website: [www.saarc-sec.org](http://www.saarc-sec.org)

b. The North Atlantic Treaty Organization (NATO)

Website: [www.nato.int/cps/en](http://www.nato.int/cps/en)

## 6. United Nations and Affiliated Bodies

All reports or documents from the United Nations, its organs or affiliated bodies may be considered as a credible source of information.

Website: [www.un.org](http://www.un.org).

a. Organs such as-

i. UN Security Council - [www.un.org/Docs/sc/](http://www.un.org/Docs/sc/)

ii. UNGA [www.un.org/en/ga/](http://www.un.org/en/ga/)

b. UN Affiliated bodies such as,

i. The International Atomic Energy Agency (IAEA) [www.iaea.org](http://www.iaea.org)

ii. The World Bank (WB) [www.worldbank.org](http://www.worldbank.org)

## **Use of AI is strictly prohibited**

**If you are found using AI tools for speeches or research, you will be removed from the committee. For research and preparation, it is strongly recommended that you use only the credible sources listed above.**



## Definition and Digital Platform Analysis

### Definition:

There is no international definition of cybercrime or cyberattacks. Offences typically cluster around the following categories:



Offences against the confidentiality, integrity and availability of computer data and systems;

- Computer-related offences;
- Content-related offences;
- Offences related to infringements of copyright and related rights.

Broadly, cybercrime can be described as having cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child abuse.

- Cyber-dependent crime requires an information and communications technology infrastructure and is often typified as the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure (e.g. the cyber-takeover of a power-plant by an organised crime group) and taking a website offline by

overloading it with data (a DDOS attack).

- Cyber-enabled crime is that which can occur in the offline world but can also be facilitated by information and communications technology. This typically includes online frauds, purchases of drugs online and online money laundering.

### Platform data:

Social Media: Instagram leads with approx. 29.8% of cyberbullying incidents, followed by Facebook at 26.2%, and Snapchat at 22%

Online messaging platforms: Platforms generally used for the purpose of collaborating while gaming like discord, usually lead to online cyberbullying via text message or voice chat

Anonymous Platforms: Anonymous posting sites create environments where perpetrators feel empowered (reddit)

### **Gender and Identity-Based Targeting**

Violence online that threatens girls and women with harassment and killing has been employed to intimidate them and has been found to result in significant psychological trauma, causing loss of confidence and self-exclusion from the internet. Subsequently, this can restrict girls from accessing educational, social, and political opportunities. In a single international poll, 38% of girls reported being harassed or abused online and 24% of those who reported being harassed stated it occurred on a social network site.

### **International Initiatives**

#### **Convention on the Rights of the Child (CRC) (1989)**

The CRC serves as the primary international legal framework that outlines the rights of children throughout the world. Article 19 of the convention requires State Parties to take measures to shield children from any violent acts. The abuse mentioned here includes the psychological kind as well as cyberbullying. The Committee on the Rights of the Child's General Comment No. 13 points directly to cyberbullying as one of the issues covered in the document; it also suggests implementation of educational measures, providing information on self defense, empowering children, and finally, States taking most of the responsibility.

#### **Council of Europe Convention on Cybercrime (Budapest Convention)**

The Budapest Convention, the first worldwide treaty on internet related crimes, promotes the legal harmonization of national laws to fight against the usage of the internet for inhumane acts upon children, online grooming and the spread of illegal material.

#### **United Nations Guiding Principles on Business and Human Rights (2011)**

Ones principles state that the business sector has a responsibility to show respect for human rights which include online rights of children. Companies are urged to refrain from committing violations and enable digital activities to be a source of no harm to children.

### **Artificial Intelligence: Dual use technology in cyberbullying**

### **Negative Duality of AI:**

Artificial Intelligence (AI) is a powerful tool that has a lot of potential but also a major risk kind of tool when it is misused for cyberbullying purposes. By the use of deepfake videos, automated harassment bots, and fake accounts that spread misinformation or targeted abuse, AI can amplify the hateful behaviour to a level no one can imagine. Wrongdoers could take advantage of the AI algorithms to find the most vulnerable persons and then trick social media algorithms to make hateful content reach more people. The use of such tools not only results in the emotional suffering of individuals but also poses a threat to their privacy, giving them the freedom to express themselves, and social harmony. The possibility of AI-facilitated cyberbullying calls for cooperation and regulation at the highest international level without further delay.

### **Positive Duality of AI:**

On the other hand, AI may be a necessary weapon in the fight against cyberbullying. By means of sophisticated machine learning models, the AI systems are locating and identifying that which is in poor language, hate speech, and the production of harmful content on the communication platforms with great accuracy. Thus, the intervention of the moderators can be timely, and the means for the support of the victims can be opened. Besides that, AI-driven educational instruments and conversational agents provide a supply of awareness raising and the promotion of responsible behaviour on the internet, which is the most effective way of protecting children and other vulnerable groups. The United Nations considers such beneficial uses as the main elements of the construction of safer digital spaces.

### **Ethical Oversight Challenges:**

The ethical oversight issues when using AI to tackle cyberbullying are quite a large and complex assortment of problems. Most importantly, the AI should be able to detect the harmful content in a way that respects privacy rights, is free from biases, and does not infringe on freedom of expression. Transparency about how the AI algorithms function, taking responsibility for the situations in which the system errs or is used improperly, and ensuring that discrimination is not aggravated are still the main issues that concern the Member States. Moreover, the swift development of AI technologies makes the challenges even more difficult and demands from the regulatory frameworks to be flexible and that policymaking to be inclusive of the different stakeholders, children among them. The difficult balancing of efficient cyberbullying prevention and respect for fundamental rights is a complex issue which, nevertheless, can be resolved if there exist sound ethical principles and worldwide collaboration.

# Case studies

## Discord Data Leak 2025

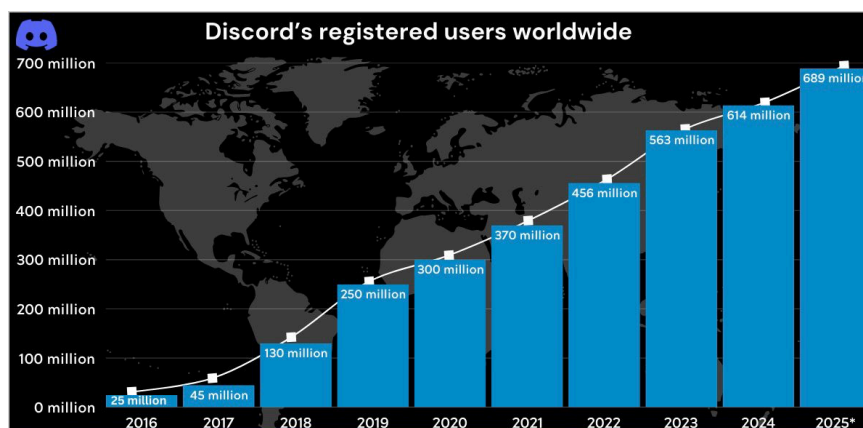
Discord, in October 2025, announced a significant data breach that impacted about 70,000 users. The breach was due to a security hole in a third-party vendor (5CA) that provides customer support. The intruders got hold of 1.5 terabytes (TB) of sensitive data via the Zendesk platform linked with Discord during a 58 hour hacking session. Among the data that went out were pictures of people's government IDs, their real names, and emails, making it one of the largest

privacy breaches of the platform.

### Key Findings:

Cause: Supply chain cyberattack through the compromise of third-party vendor credentials.

Data Exposed: 70,000 ID photos, over 1.5 TB of data, including support transcripts.



Duration: 58 hours from the time of the incident to the detection and containment of the breach.

Impact: The personal data of users in more than 50 countries was compromised, and they are now at risk of identity theft.

### Response Actions:

After the incident, Discord quickly severed the vendor's system access, informed the affected users, and started collaboration with EU cyber authorities and US-based security partners. Also, the company has improved vendor security audits and put in place AI-based threat detection systems for security enhancement and to prevent similar occurrences.

### Global Implications:

Emphasises the increasing security risks associated with third parties in the digital ecosystem.

It questions the trade-off between data verification and user privacy protection.

As a result of this incident, discussions about policies have been initiated in tech regulatory forums and the UN digital safety initiatives under the Global Digital Compact (2025) framework.

### Conclusion:

The Discord 2025 Data Leak is a wake-up call that cyber risks are deeply intertwined; a platform that is secure on its own may still be exposed via its external partners. It conveys the message that there is an urgent need for more robust worldwide cybersecurity management, vendor

trustworthiness, and clear data protection norms in a world that is increasingly reliant on technology.

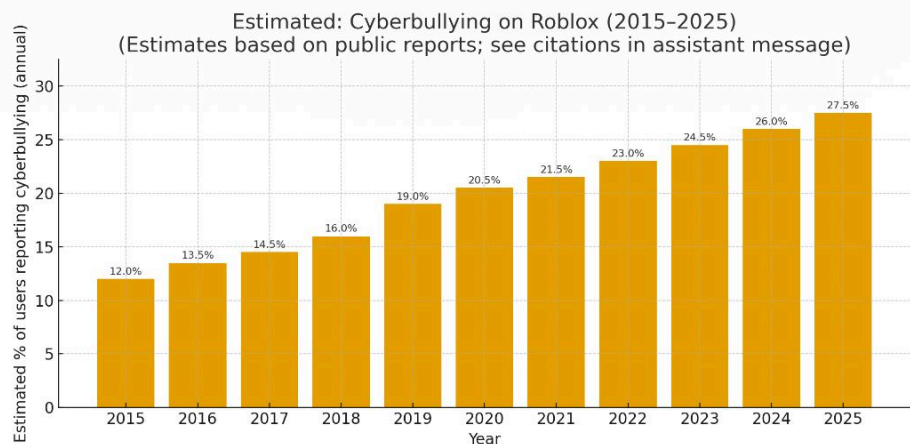
## **Cases of online bullying in Roblox**

Roblox is one of the world's most popular online gaming platforms, especially among children. It allows users to create their own games and virtual worlds, play games made by others, and interact with millions

of players worldwide. As of 2025, Roblox has over 85 million daily active users, with approximately 40-53% of its users being children under the age of 13

The platform is marketed as a “safe”

creative space for children where they can build, play, and socialise. However, behind this family-friendly image lies a growing crisis: Roblox has become what many experts, parents, and law enforcement officials now call a "digital hunting ground" for online predators



### **Case 1: Texas Home Invasion**

A 13-year-old girl from Galveston, Texas, was tricked and lured by her online friends on Roblox, who were actually 25 and 28, respectively. These men tricked her for months by posing as her friend, and in-game, she used her mother’s banking details to purchase items. These men stole these details and scammed her parents out of over \$30,000. Such cases have recently sprung up all across Roblox, especially among those who are below 13.

### **Case 2: Charleston County Exploitation**

An 11-year-old girl from Charleston County, South Carolina, was targeted by a group of online gaming friends. She was repeatedly bullied and insulted over the span of 6 months. She suffered immense mental stress and trauma, affecting her studies and social life. Her friends on the online gaming group were 18 and 21 and had a long-standing record of targeting younger kids and verbally insulting and bullying them.

## **What Critics Say**

### **1. Prioritising Profit Over Safety**

- a. Multiple lawsuits accuse Roblox of prioritising growth and profit over child safety
- b. The company benefits financially from predators because it takes a cut from all Robux transactions, including when predators use Robux to groom children

### **2. Inadequate Safety Measures**

- a. No meaningful age verification system. Easy for banned users to create new accounts
- b. Filters can be easily bypassed. Predators can use third-party apps to communicate with children, making Roblox's chat filters useless

### **3. Misleading Marketing**

- a. Roblox markets itself as a safe platform for children, leading parents to trust it
- b. Parents feel betrayed when they discover the reality of the dangers

## **Questions to consider**

1. How can the international community enhance cooperation and coordination among states, regional bodies, and technology platforms to create effective legal and policy frameworks that prevent, detect, and respond to cyberbullying across diverse jurisdictions?
2. What comprehensive strategies can the UN introduce to empower victims of cyberbullying, including the development of victim support systems, educational programs on digital safety, and promotion of inclusive online environments that respect human rights and dignity?
3. Technology companies don't seem to care about online bullying and harassment. What are ways to keep them accountable?
4. In what ways could Member States ensure a high level of protection for individuals against cyberbullying, at the same time, respecting the freedom of expression and the privacy rights online?
5. What kind of systems could be put in place to allow a timely and efficient way of communication and intervention in the cases of cyberbullying, that is, incidents that involve children?

6. In what ways could the support of families, teachers and local communities be better used for the prevention of cyberbullying and to mitigate it?

7. What kind of initiatives should, for example, the United Nations take to facilitate coordination among different countries in terms of gathering data and conducting research about the worldwide impact of cyberbullying?

