

BTUMUN'26
UNHRC STUDY GUIDE

Committee: UNHRC (United Nations Human Rights Council)

Agenda Item: AI in Cybersecurity Mass Surveillance and Human Rights Implications

President Chair: İris Eren

Co-Chair: Melisa Mutlu

1. Letters from Chairs

Esteemed Delegates,

It is our distinct honor to welcome you to the UNHRC (United Nations Human Rights Council) Committee. As the Chair and the Co-Chair, we wish you an amazing conference at BTUMUN'26!

As you prepare for this conference, we expect each delegate to uphold the principles of diplomacy, integrity, and intellectual rigor that define Model United Nations. The UNHRC (United Nations Human Rights Council) Committee requires not only comprehensive research and human rights awareness, but also the ability to negotiate, draft effective resolutions, and engage in constructive debate. Delegates are encouraged to thoroughly understand their assigned country's foreign policy, strategic interests, and past actions regarding the agenda items. During committee sessions, professionalism must remain paramount. Respect for fellow delegates, adherence to parliamentary procedure, and the pursuit of feasible, well structured solutions will be essential.

Remember that diplomacy is not the art of speaking the loudest, but the skill of building consensus through reasoned argumentation and compromise. We trust that you will approach this conference with dedication and determination. May your preparations be thorough and your participation exemplary. We look forward to witnessing your contributions in committee!

Sincerely,

UNHRC Chairs.

Chair: İris Eren

Co-Chair: Melisa Mutlu

Gmail: iriseren2008@gmail.com

Gmail: melisamt109@gmail.com

Whatsapp: +905322247144

Whatsapp: +905523420474

2. Preface

Recalling the purposes and principles of the Charter of the United Nations, including the promotion of international peace and security and the promotion of fundamental human rights and freedoms,

Reaffirming the Universal Declaration of Human Rights in particular article 12 on the right to privacy and article 19 on freedom of expression and access to information,

Having regard to the International Covenant on Civil and Political Rights protecting fundamental rights, such as privacy, liberty and security of person in the context of evolving technologies,

In aware of the rapid development and increasing use of artificial intelligence in the area of cybersecurity, enhancing the capacities of States to detect, prevent and respond to cyber threats and digital risks,

Recognizing the immense benefits of AI powered systems to improve cybersecurity architectures, increase threat intelligence, and support law enforcement, deeply concerned that the growing use of AI powered mass surveillance tools, including facial recognition and large scale data collection, may result in unlawful interference with privacy and the suppression of fundamental freedoms,

Alarmed by the lack of comprehensive and universally accepted regulatory frameworks, which increases the risk of misuse in the absence of transparency, accountability, and effective oversight,

Acknowledging the role of the United Nations Human Rights Council in addressing emerging challenges posed by new technologies, human rights compliant innovation, emphasizing the need for a balanced approach allowing the effective use of AI in cybersecurity with full respect for international human rights obligations and recognizing the importance of international cooperation, multi-stakeholder engagement and inclusive governance in the development of transparent and accountable frameworks.

Stressing the urgent need to protect democratic values, prevent the abuse of surveillance technologies and ensure that the applications of AI remain consistent with the principles of legality, necessity, proportionality and accountability.

3. Introduction to the Committee

The United Nations Human Rights Council (UNHRC) is an intergovernmental body within the United Nations system which is responsible for the promotion and protection of all human rights around the globe. The Council was established for the purpose of dealing with cases of violations of human rights and making recommendations, and plays an important part in increasing international cooperation and ensuring the protection of fundamental freedoms in conformity with international law.

The convergence of Artificial Intelligence (AI) cybersecurity and mass surveillance has become a major global issue in today's rapidly changing digital world. The emergence of AI-driven technologies has greatly improved security capabilities, data analysis, and threat detection, but has also raised serious concerns about the protection of individual privacy, freedom of expression and the potential for misuse by state and non-state actors alike.

The spread of AI-enabled surveillance systems if not regulated with a view to transparency, accountability and respect for international standards, risks eroding fundamental human rights principles.

As part of this agenda, the Council aims to critically evaluate the implications of AI in cybersecurity frameworks and mass surveillance practices, ensuring that technological progress does not come at the expense of fundamental human rights and civil liberties.

In addition to the expanding security applications, AI has been deeply integrated into modern cybersecurity systems, enabling governments and institutions to detect cyber threats, prevent large-scale attacks, and analyze massive volumes of digital data in real time. Yet these same technologies have also contributed to the intensification of mass surveillance practices such as facial recognition, predictive policing, and broad data collection without explicit consent. These developments have spurred global debate over the trade-off between national security and individual privacy rights.

Therefore, it is increasingly important that ethical frameworks and legal safeguards are put in place by the international community to ensure that AI is used responsibly, transparently and in full compliance with human rights standards.



4. Definition of Key Terms

Mass Surveillance

The large scale monitoring of populations through digital and physical technologies. It raises concerns regarding privacy and state control.

Cybersecurity

The protection of digital systems, networks, and data from cyberattacks and unauthorized access, often enhanced by AI technologies.

Data Privacy

The right of individuals to control how their personal data is collected, stored, and used. It is a key human rights issue in the digital age.

Digital Rights

Rights that protect individuals in the digital space, including privacy, freedom of expression, and access to information.

State Surveillance

Government monitoring of citizens for security or intelligence purposes which often creates tension between security and civil liberties.

Cyber Threats

Potential dangers to computer systems such as hacking, malware, phishing, and ransomware attacks.

Human Rights Violation

Any action that infringes upon fundamental rights such as privacy, freedom of expression, and protection from unlawful surveillance.

Predictive Policing

A data driven policing method that uses AI to predict potential criminal activity or high-risk areas that may reinforce bias in law enforcement.

Biometric Data

Unique biological characteristics such as fingerprints, iris patterns, or facial features used for identification and tracking.

Privacy Invasion

Unauthorized access or monitoring of a persons personal life, data, or communications.

5. History of UNHRC

The United Nations Human Rights Council (UNHRC) was established on 15 March 2006 by the United Nations General Assembly through Resolution 60/251 as part of the broader reform of the UN system. The Council was tasked with monitoring and preventing human rights abuses around the globe.

Its design included provisions to ensure that it is a more accountable and transparent body with stronger institutional framework than was its predecessor. The number of members is 47, elected by the UN General Assembly and based on geographical distribution, with members serving for three years, and can be suspended if gross and systematic human rights violations occur. One of its most important innovations is the Universal Periodic Review (UPR), which was introduced in 2007 and ensured that all UN Member States, rather than some chosen ones, would be reviewed on their human rights performance in a regular and fair cycle, ensuring that they are equally subjected to such reviews.

The Council works through regular meetings held in Geneva, Switzerland, during which it deals with urgent human rights situations, issues resolutions, and appoints Special Rapporteurs as well as Independent Experts with mandates to examine specific situations. UNHRC has since made remarkable achievements in conflict management, protection of freedom of expression and speech, management of discrimination and response to emerging global human rights issues.

In recent years, the Council's mandate has been broadened to include discussions on contemporary technological advancements and their implications on human rights. Relevant issues regarding the policies on artificial intelligence, mass surveillance, digital privacy, and cybersecurity are some of the areas central to its agenda. Such topics demonstrate a demand for international regulation of technological progress so that basic human rights such as privacy, dignity, and freedom of expression are not violated.

Today, the UNHRC continues to serve as the primary UN body that is responsible for nurturing and protecting human rights across the world, though it has also shifted its focus to address the human rights violations present in the digital and interconnected world.

6. How the Council Works

The Human Rights Council meets for at least 10 weeks per year at human rights issues. The United Nations Office in Geneva, Switzerland, in regular sessions usually taking place in March, June and September. The Council can also convene urgent meetings on short notice to respond to emerging human rights crises – 28 such special sessions were held thus far.

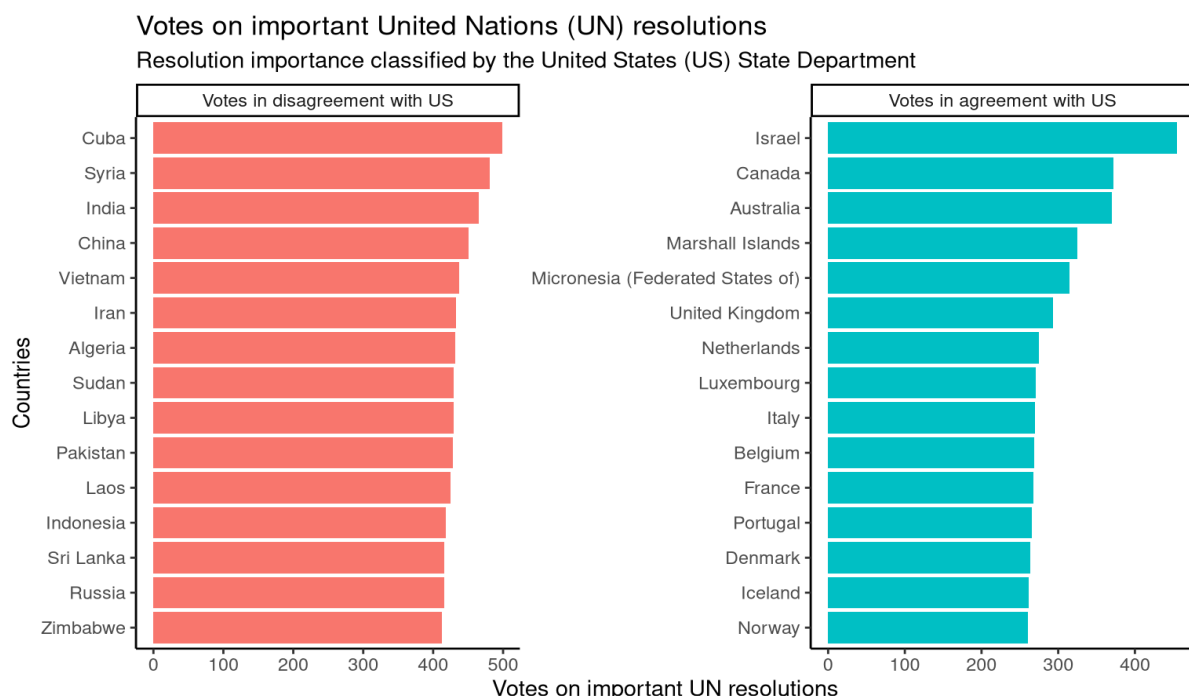
The Council's subsidiary bodies meet for approximately 20 additional weeks each year. Since its 1st session in 2006, the Council's agenda has been expanding and its meeting time has more than doubled. The Council is made up of 47 member States who are elected by the UN General Assembly by a simple majority vote, through a secret ballot. Members of the Council are elected for three year terms with one third of the members being renewed each year.

Council membership is based on equitable geographical distribution of seats according to the following regional breakdown: 13 African States; 13 Asia Pacific States; 8 Latin

American and Caribbean States; 7 Western European and other States; 6 Eastern European States. 117 countries have served as Council members so far, reflecting the UN's diversity giving it legitimacy when speaking out on human rights violations in all countries.

The Council has a Bureau which consists of a president and four vice-presidents who represent each of the five regional groups, and who serve for a year in accordance with the Council's annual cycle (January – December). Staff from the Office of the High Commissioner for Human Rights (OHCHR) serve as the secretariat for the Council providing its members with technical, substantive and administrative support.

In addition to the member States of the Council, observers, which include non-member States, inter-governmental organizations, national human rights institutions, and non-governmental organizations (NGOs), also participate actively in Council sessions.



7. Major Countries Involved

A. United States of America (USA)

The United States is one of the most influential actors in AI development, cybersecurity infrastructure, and global intelligence operations. It hosts major technology companies such as Google, Microsoft, and Meta, which play a key role in AI driven data analysis and surveillance technologies. The US intelligence community operates extensive surveillance programs through agencies such as the NSA, which were revealed by the 2013 Snowden leaks to have collected bulk metadata from millions of individuals globally. According to various cybersecurity reports, the US allocates over \$15 billion annually to federal cybersecurity programs. While the country emphasizes national security and counter terrorism, it is also a strong advocate for digital innovation, though frequently criticized for privacy concerns and mass data collection practices.

B. China

China is a global leader in artificial intelligence and large scale surveillance systems, particularly in facial recognition, social credit systems, and predictive policing. It is estimated that China has over 700 million surveillance cameras installed nationwide, making it one of the most heavily monitored societies in the world. The government integrates AI into public security systems to enhance social stability and crime prevention. Companies such as Huawei and Hikvision are key players in surveillance technology development. However, international human rights organizations frequently raise concerns regarding digital privacy, lack of consent, and extensive state monitoring of citizens, particularly in sensitive regions.

C. United Kingdom (UK)

The United Kingdom plays a significant role in global cybersecurity cooperation and intelligence-sharing networks, particularly through the “Five Eyes” alliance alongside the US, Canada, Australia, and New Zealand. London is considered one of the most surveilled cities in Europe, with an estimated more than 500,000 CCTV cameras operating across the city. The UK government invests heavily in cyber defense, with its National Cyber Security Centre (NCSC) leading national strategies against cyber threats. While the UK supports strong security frameworks, it also faces criticism regarding surveillance expansion and the balance between security and civil liberties.

D. Germany

Germany is widely recognized for its strong emphasis on data protection, digital rights, and privacy regulations. Influenced by its historical experiences with authoritarian surveillance regimes, Germany is one of the most privacy conscious countries in the world. As part of the European Union, it strictly enforces the General Data Protection Regulation (GDPR), which

impacts over 450 million EU citizens and is considered one of the strongest data privacy laws globally. Germany also actively participates in AI ethics discussions and promotes the development of transparent and human rights compliant AI systems. However, it continues to face challenges in balancing cybersecurity needs with strict privacy laws.

E. Russia

Russia plays an active role in cyber operations, information control, and state led surveillance systems. The country has developed extensive digital monitoring capabilities and is often associated with cyber warfare activities and state sponsored cyber operations targeting both domestic and international entities. Russia has been linked to several high profile cyber incidents in recent years, with cybersecurity firms reporting thousands of politically motivated cyberattacks originating from or associated with Russian networks annually. Internally, the government maintains strict control over internet infrastructure and digital communication platforms, raising concerns regarding freedom of expression and digital rights.

F. France

France is a key European actor in cybersecurity policy, AI regulation, and digital governance. It has significantly increased investment in cybersecurity, allocating approximately €1 billion under its national cybersecurity strategy (2020–2025). France also plays an active role in shaping European Union regulations on artificial intelligence and data protection. The country supports the development of “ethical AI” frameworks that ensure transparency, accountability, and respect for human rights. At the same time, France has expanded surveillance measures for counter terrorism purposes, especially after major security incidents, which has sparked debate about the balance between public safety and privacy rights.



8. Background Information

The United Nations Human Rights Council (UNHRC) is the principal UN body for the promotion and protection of human rights worldwide. It was established on 15 March 2006 by the United Nations General Assembly by Resolution 60/251 to replace the former UN Commission on Human Rights, which had been criticized for politicization and inconsistent treatment of human rights violations.

The Council has 47 Member States, elected for three-year terms by the General Assembly of the UN on the basis of equitable geographical distribution. Members have to maintain high human rights standards and membership of a state can be suspended by a two thirds majority vote of the General Assembly in the event of gross and systematic violations.

One of the most important procedures of the UNHRC is that of the Universal Periodic Review (UPR), which was created in 2007. This procedure involves the review of all 193 UN member states about their human rights activities every 4.5 years; this way, all states are treated equally without regard to politics or economy. The Special Procedures involve more than forty Special Rapporteurs and Independent Experts that investigate human rights situations in specific countries and on particular issues.

The UNHRC works at least three sessions per year in Geneva, Switzerland. It can also organize emergency special sessions to discuss and address urgent human rights issues. This body deals with many aspects, such as freedom of speech, discrimination, wars, and protection of minority groups and refugees.

The Council in recent times has paid special attention to global problems of the modern era, mainly due to the increasing role of technology in human rights. With over 5 billion people using the Internet globally, the problems of artificial intelligence, surveillance, cyber security, and digital privacy are now major concerns of the council.

In today's world, the UNHRC continues to be an important international forum for discussion, dialogue, accountability, and collaboration, ensuring the respect of human rights in both the old and new global worlds.

9. Qarma

1. Motion for the use of facial recognition technology in public surveillance systems.
2. Motion for the protection of digital rights under international law.
3. Motion to talk about the risks of mass surveillance to freedom of expression.
4. How the biometric data collection affects human rights violations?
5. Motion for a moderated caucus on international regulation of Artificial Intelligence in surveillance systems.
6. How to strengthen the international frameworks for data protection?
7. Motion for a moderated caucus on the right to privacy in the digital age.
8. How to develop international cooperation against cyber warfare and cyber attacks?
9. How can we protect critical infrastructure from AI driven cyber threats?
10. Motion for a moderated caucus on safeguarding human dignity in AI powered surveillance systems

10. Bibliography

<https://www.unhcr.org/>

https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/HRC_booklet_EN.pdf

[https://ENSZ.70_eredmények és kudarcok.jpg](https://ENSZ.70.eredmenyek.es.kudarcok.jpg)

[https://110 millions de personnes déplacées de force, un nouveau record.jpg](https://110.millions.de.personnes.deplacées.de.force.un.nouveau.record.jpg)

<figure1-1.png>

https://www.ohchr.org/en/ohchr_homepage

[https://en.wikipedia.org/wiki/United Nations Human Rights Council](https://en.wikipedia.org/wiki/United_Nations_Human_Rights_Council)

<https://www.britannica.com/topic/human-rights/The-UN-Commission-on-Human-Rights-1946-2006-and-the-UN-Human-Rights-Council>

<https://research.un.org/en/undhr/draftingcommittee>

<https://www.un.org/en/about-us/universal-declaration-of-human-rights>