STUDY GUIDE

GA4: SPECPOL

15-17 MAY

BAALMUN'26

Table of Contents

Letter from the Secretaries-General

Dear Distinguished Guests,

As the Secretaries-General of BAALMUN'26, it is our great pleasure to welcome you to the 4th edition of BAALMUN. We are honoured to host you at our conference, which will take place between the 15th and 17th of May at our school.

We have worked tirelessly to organize a conference that offers unique opportunities and brings students together under the ideals of Model United Nations. Our conference aims to create an environment where delegates can engage in fruitful debates, develop diplomatic skills, and collaborate to address some of the most pressing global issues of our time. The academic team has carefully designed the committees and topics to reflect and uphold these ideals.

We would also like to highlight the hard work that our team has put in to provide you with the best possible MUN experience. Over the past months, the academic and organizing teams have worked tirelessly to ensure the quality of our conference. Their dedication and commitment have played a crucial role in making BAALMUN 2026 possible, and we are incredibly grateful for their efforts.

Lastly, we hope that you will enjoy our conference and that it will provide you with new knowledge and unforgettable memories. We wish you a wonderful time and look forward to welcoming you soon.

Best regards,
The BAALMUN’26 Secretariat

Letter from the Co-Under Secretaries-General

Dear Secretariat, distinguished delegates and honourable guests,

It is a great honour for me to address you as the Under Secretaries-General of this committee.

On behalf of both my school’s MUN club and the delegates, I would like to express my gratitude for upholding the academy and organisation of this conference. Having witnessed firsthand the challenges you faced during the preparation of this conference, watching you tackle those hurdles and exercise your co-working skills was both deeply instructive and impressive.

We have organised this committee and guide for those who wish to gain insight and achieve mastery in committees like SPECPOL-GA5 or the other variants of committees throughout your Model United Nations career.

If you have any questions or wish to reach out, please feel free to contact me via email, and I hope for a great conference for everyone

Candid regards,

Neva Çetin - Taym Al-Qassab

Under-Secretaries General

Introduction to the Committee

The Special Political and Decolonization Committee, commonly referred to as the Fourth Committee or SPECPOL, is one of the six main committees of the United Nations General Assembly. Rooted in the post-World War II mandate for decolonization and the international trusteeship system established under Article 16 of the UN Charter, the committee was originally tasked with overseeing the transition of non-self-governing territories toward independence.

However, as the global political landscape evolved, so too did SPECPOL's remit. Today, the committee handles a diverse and complex portfolio that spans beyond its colonial origins to include "special political" questions such as international peacekeeping operations, the effects of atomic radiation, and the peaceful uses of outer space.

Besides, it maintains critical oversight of the United Nations Relief and Works Agency (UNRWA) and continues to provide a unique platform for petitioners from territories still seeking self-determination by balancing legacy issues of sovereignty with contemporary

challenges in information governance and regional security. SPECPOL remains a vital forum for addressing some of the world's most sensitive political and humanitarian concerns.

1. Introduction to the Agenda Item

The rapid integration of Artificial Intelligence (AI) and network-based surveillance into state-sponsored operations represents a transformative shift in global security, governance, and human rights. Once the domain of science fiction, algorithmic targeting, predictive policing, and autonomous intelligence systems are now active pillars of national security architectures. These technologies offer states different capabilities for accuracy and efficiency, but they also introduce severe ethical dilemmas concerning accountability, civilian protection, and the erosion of digital sovereignty. As the lines between civilian and military infrastructure blur, the Fourth Committee (SPECPOL) faces a critical command: to navigate the "special political" implications of a data-driven world where algorithms can determine the life-and-death decisions of a sovereign state.

The urgency of this discussion is underscored by the contemporary landscape of warfare and hybrid operations. In the escalating confrontation between Iran and Israel, for instance, the world has witnessed the transition to what many analysts term the "First AI War." From the deployment of advanced algorithmic targeting systems and integrated air defense suites to the use of asymmetric cyber-surveillance and autonomous drone swarms, these conflicts serve as a live laboratory for modern digital warfare. Events such as targeted drone strikes and the compromise of networked communication systems verify that surveillance is no longer merely a tool for observation but a kinetic instrument of state power.

This agenda item challenges the committee to establish international norms that balance the security needs of states with the fundamental rights of individuals in an era where the battlefield is increasingly defined by code rather than geography.

2. Key Terms and Definitions

Predictive Law Enforcement: The use of AI and data analysis to predict where crimes may happen or who may be involved in criminal activity before a crime occurs.

Biometric Identification: The technology that recognizes people through unique physical features such as fingerprints, eye scans etc.

Behavioural Profiling: The process of studying a person's actions, habits, or online activity to predict their behaviour or identify possible risks.

Automated Threat Detection: The use of computer systems and AI to automatically detect possible dangers, suspicious activity or security threats.

Surveillance Infrastructure: The systems and technologies used for monitoring people and communications such as CCTV cameras, internet tracking systems and data collection networks.

Transnational Pressure: Political, economic, or digital pressure applied by one state across national borders to influence another country or people living abroad.

Exiles: People who are forced to leave their home country, often for political or security reasons.

Algorithmic Diaspora: The way governments, companies, or online platforms use algorithms and digital technologies to monitor, influence, or track diaspora communities through social media, online activity, and data collection across borders.

Mass Surveillance The systematic and large-scale monitoring of entire populations or large segments of a society by governments or their sponsored agencies, usually without any individualized suspicion or judicial oversight. Mass surveillance, however, is a blanket collection of data, not targeted. It collects communications, movements, financial transactions, online behavior, and more, and stores them for analysis by AI-powered tools.

Predictive Policing **Analyzing historical crime data, behavioral patterns, and demographic information using algorithms and AI systems to predict where crimes might occur or who might be a perpetrator. Predictive policing aims to prevent crime before it happens, rather than respond to it after the fact, and this raises serious issues about self-fulfilling prophecies, racial bias and punishing people for things they haven't yet done.**

Facial Recognition Technology (FRT) It is an AI-powered biometric identification system that looks at the unique geometric features of an individual's face and compares them to a database of stored images. FRT can be applied to live video feeds in real time, or retrospectively on recorded footage. It is used for security and identity verification, but it raises major concerns around accuracy disparities across racial groups, mass surveillance enablement, and the lack of consent from individuals being scanned.

Due Process A fundamental legal principle – enshrined in instruments such as Article 14 of the ICCPR – which guarantees that individuals are entitled to fair, transparent and impartial procedures prior to the state taking any action affecting their rights, liberty or property. In the context of AI surveillance, due process is a threat because algorithmic decisions can result in arrest, restriction, or punishment without human review, clear legal basis, or ability to contest the decision made against the individual.

Data Sovereignty The principle that data created within a country's borders or by its

citizens falls under the legal, regulatory, and governance frameworks of that country and cannot be accessed, transferred, or processed by foreign entities without explicit consent or legal authorization. Authoritarian states use the concept of data sovereignty to insulate domestic surveillance from international scrutiny, and developing countries use it to prevent the foreign exploitation of their citizens' data in AI surveillance contexts.

Zero-Day Exploit

A cybersecurity vulnerability in software or hardware that is unknown to the vendor or developer, i.e. there is no patch or fix available at the time of discovery. These vulnerabilities are exploited by governments and state-sponsored actors to secretly access target devices. The most famous example is Pegasus spyware that used zero-day exploits in iOS to silently access journalists' and activists' phones without any interaction from the victim. A zero-day is so called because developers have had zero days to fix the flaw.

Digital Authoritarianism

A governance model in which states use digital technologies – including AI surveillance, social media monitoring, internet censorship and biometric tracking – to consolidate political control, suppress dissent and manipulate public discourse. Traditional authoritarianism relies on the physical coercion of citizens, while digital authoritarianism operates largely invisibly, exerting a chilling effect on free expression that does not require mass arrests or overt violence. Frequent examples include China's surveillance apparatus in Xinjiang and Iran's shutdown of the internet during protests.

Export Controls

Restrictions or controls imposed by governments on the transfer of certain technologies, goods or software to foreign persons or countries, usually for reasons of national security or human rights. As for AI surveillance , one proposed solution is to impose export controls to prevent authoritarian regimes from buying surveillance technology developed in democratic states . The EU, U.S. and members of the Wassenaar Arrangement have discussed broadening export control regimes to cover dual-use surveillance technologies like facial recognition systems and IMSI catchers.

Transparency Obligation

A legal or normative requirement for governments or corporations to disclose the design, training, deployment and usage of AI systems, especially when such systems impact upon the rights of individuals. In surveillance scenarios, transparency obligations would include public disclosure of when and how AI-enabled monitoring tools are deployed, what data is collected, how long it is retained, and what oversight mechanisms are in place. Transparency is a key governance principle mentioned in both the EU AI Act and the UN's report on Governing AI for Humanity.

Accountability Gap

No clear legal liability or ramifications for AI systems that cause harm, make incorrect decisions, or enable human rights abuses. In government surveillance contexts, the accountability gap occurs because automated systems make decisions—flagging individuals, denying services, or initiating

investigations—without a clearly identifiable human decision-maker to hold responsible. This problem is especially acute when surveillance technology is purchased from private companies under trade-secret protections that keep operational details hidden even from parliamentary oversight.

3. Background and Historical Context

The relationship between state power and surveillance is not a product of the digital age. For centuries, governments have monitored populations to maintain security, control opposition, and collect intelligence. In the past, this relied mainly on human informants and secret police organizations such as the KGB in the Soviet Union and the Stasi in East Germany. During the Cold War, surveillance became more technological through signals intelligence systems like ECHELON, which allowed allied countries to intercept communications on a large scale. However, these systems were still limited by the need for human analysis and mainly focused on foreign threats.

The spread of the internet and digital technologies in the 1990s and 2000s completely changed the scale of surveillance. As communication, banking, and daily activities moved online, governments gained access to enormous amounts of personal data. After the September 11 attacks in 2001, many states expanded surveillance powers in the name of national security. Laws such as the USA PATRIOT Act increased the authority of intelligence agencies to collect and monitor digital communications. The debate became even more intense in 2013 after Edward Snowden revealed programs such as PRISM and XKeyscore, showing that governments were conducting large-scale data collection from global technology platforms.

At the international level, AI and network-based surveillance have become major tools of modern state power and conflict. Spyware technologies such as Pegasus have reportedly been used against journalists, activists, and opposition figures in many countries. In recent years, the confrontation between Iran and Israel has also demonstrated how cyber operations, AI-supported surveillance, and digital intelligence are now central parts of geopolitical rivalry. Both states have used hacking operations, signals intelligence, drone surveillance, and online information campaigns to weaken each other without always crossing into direct military conflicts.

Today, artificial intelligence has made surveillance faster, more automated, and more precise. Facial recognition systems, predictive policing algorithms, and AI-supported data analysis are now widely used by both authoritarian and democratic governments. China’s surveillance systems in Xinjiang, including biometric monitoring and facial recognition, have faced strong international criticism. At the same time, countries such as the United Kingdom and the United States have also expanded AI-based surveillance through CCTV networks, facial recognition trials, and data integration systems used by law enforcement agencies. Critics argue that predictive policing technologies can reinforce ethnic and social biases since they rely on historical crime data.

Despite the rapid growth of these technologies, there is still no connection upon the international framework regulating AI surveillance and cyber operations. This creates serious concerns about privacy, human rights, misinformation, and the militarization of digital technologies. As surveillance capabilities continue to expand, the international community faces the difficult challenge of balancing national security needs with the protection of civil liberties and international law.

4. Current Global Situation and Statistics

4.1. Current Global Situation

AI-powered surveillance systems have become one of the fastest-spreading state tools of the 21st century. A growing number of states are using modern AI surveillance tools to monitor, track, and surveil citizens to accomplish a range of policy objectives — some lawful, others that violate human rights, and many of which fall into a unclear middle ground.

The Carnegie Endowment for International Peace's **AI Global Surveillance (AIGS) Index** clearly reveals the scale of this phenomenon: the index compiles empirical data on AI surveillance use for 176 countries around the world, with the purpose of showing how new surveillance capabilities are transforming governments' ability to monitor and track individuals or systems. As of 2019, at least 75 countries had employed AI technologies for surveillance purposes. Given the rapid pace of growth documented since then, this number is almost certainly significantly higher today.

This is not merely a technological issue, but a deep political and power issue. Authoritarian governments across the globe are already deploying AI surveillance and policing systems, and there is evidence that these systems are effective in quelling political dissent and entrenching existing regimes. Alarmingly, AI surveillance and policing systems have also spread across cities in the U.S. Here is the global picture, by key actors and models:

The global picture, broken down by key actors and models, is as follows

China Model: China has the world’s largest scaled state-sponsored surveillance architecture. The Chinese government has used AI extensively in sweeping crackdowns against ethnic minorities. Xinjiang and Tibet have been called “Orwellian” for their surveillance systems which include mandatory DNA samples, Wi-Fi network monitoring and omnipresent facial recognition cameras all feeding into integrated data analysis platforms. More specifically, China is using AI-powered technology to synthesize a multitude of streams of information, such as individual DNA samples, online chat histories, social media posts, medical records, and bank account information, to monitor every aspect of individuals’ lives.

Technology Exports: Surveillance technology now spreads across borders without restriction. Transfers are happening in a highly heterogeneous fashion: China is exporting surveillance technology to liberal democracies as much as it is targeting authoritarian markets. Likewise, companies based in liberal democracies — such as

Germany, France, Israel, Japan, South Korea, the UK, and the United States — are actively selling sophisticated equipment to unsavory regimes.

Developments in Democratic Countries: The problem is not confined to authoritarian regimes. Reports have surfaced about potential abuses in the U.S., including government contracts that may enable the Department of Homeland Security (DHS) to monitor social media; contractors advertise their ability to scan through millions of posts and use AI to summarize their findings for their clients.

With generative AI advancements, digital authoritarianism is entering a new phase — reinforcing autocracy and surveillance domestically, and enabling foreign interference operations externally. Unlike traditional tools of repression, generative AI models allow for more sophisticated manipulation of information and public perceptions, both at home and abroad.

4.2. Recent Statistics and Achievements

Market Size and Economic Data

- The global AI in video surveillance market was estimated at USD 6.51 billion in 2024 and is projected to reach USD 28.76 billion by 2030, growing at a CAGR of 30.6% from 2025 to 2030. This means the sector is set to more than quadruple in under five years.
- The broader market for AI in government and public services was estimated at USD 22.41 billion in 2024 and is projected to reach USD 98.13 billion by 2033, growing at a CAGR of 17.8%
- The global surveillance technology market is projected to exceed $300 billion by 2028, generating continuous pressure for deeper data access.
- The biometric technology market is expected to reach $85 billion by 2029.

Country and region data

- North America led the AI in video surveillance market with a share of 33.6% in 2024.
- The U.S. Office of Management and Budget released its 2025 Federal Agency AI Use Case Inventory, showing 3,611 individual use cases from 56 agencies, a 105% increase from the 1,757 use cases reported in 2024.
- The fastest growth rates are in the Asia-Pacific region. China, Japan and South Korea are deploying AI in surveillance, including widespread use of facial recognition technology for public security and law enforcement and use of AI-powered surveillance cameras in railway stations.

International Regulatory Developments

- The proliferation of surveillance technology has prompted some regulatory responses. The EU AI Act, provisionally approved in December 2023 and passed by the European Parliament in March 2024, seeks to protect "fundamental rights, democracy, the rule of law and environmental sustainability."Banned applications include social scoring, emotion recognition in workplaces and educational institutions, and biometric categorization systems.

However, the EU AI Act bans some uses such as real-time facial recognition in public spaces and emotion detection at work, but most of the world operates without such restrictions

Commercial Spyware: The Pegasus Case

State-sponsored surveillance extends well beyond camera-based systems — commercial spyware is an integral part of this landscape. Israel's NSO Group developed Pegasus spyware, which can be remotely installed on phones and extract everything — messages, calls, location data, camera, and microphone access. Israel uses Pegasus licenses as diplomatic currency, approving sales to countries it wants something from.The leaked Pegasus Project database contained 50,000 phone numbers concentrated in Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, and the UAE. The revelation that Pegasus had been used by governments to target journalists, activists, and opposition figures prompted international scrutiny of export licenses and led to legal responses from companies such as Apple and WhatsApp.

4.3. Possible Threats and Risky Cases

This section details the tangible dangers of AI surveillance and the documented cases of high risk that exemplify them.

Threat 1: Algorithmic Bias and Misidentification

Facial recognition systems are frequently sold as neutral tools but in practice have serious bias problems. The National Institute of Standards and Technology (NIST) study found that leading facial recognition technologies had error rates up to 100 times higher with Black and Asian faces than with white faces — disparities that too often lead to misidentifications and wrongful arrests.

These statistics have played out in real world cases.

Robert Williams became the first man in the United States to be wrongfully arrested due to a racially biased facial recognition program; law enforcement mistakenly matched security camera footage from a retail theft to Williams's driver's license photo. The charges were later dropped due to insufficient evidence.

The root cause is a basic data problem: AI-powered facial recognition programs used by law enforcement are far more error-prone on facial images of Black males than white males—a bias that stems from the lack of diversity, especially the underrepresentation of Black faces, in the datasets used to train the algorithms.

Threat 2: Eroding Democratic Institutions

AI surveillance endangers not only individuals but also the processes of democracy. AI systems can reduce the need for structural checks on executive authority and result in a concentration of power with fewer and fewer people. In the wrong hands they can assist authorities in identifying subversive behavior, discourage or punish dissent, and facilitate corruption, selective enforcement and other abuses.

We saw a concrete example of this risk in 2024.

When South Korean President Yoon Suk Yeol declared martial law and sent military troops to take over the National Assembly, they were thwarted by staffers and members of Parliament who barricaded doorways. The soldiers

did not fire on unarmed resisters — demonstrating that human judgment can still make a decisive difference. However, had that decision-making been delegated to automated AI systems, the outcome could have been very different: automated systems will not hesitate to follow orders, and shame will not prevent them from using deadly force when commanded.

Threat 3: Political Suppression and Chilling Effect

In a study published in The Quarterly Journal of Economics, researchers found that when public safety agencies acquire AI surveillance software, fewer people protest. The mere presence of these systems appears to dampen unrest. This is not merely deterrence, it is a systematic curtailment of civil liberties. The pervasive AI surveillance makes it harder to organize large-scale political action, making coups or mass protests less likely to happen.

Threat 4: Surveillance Technology Exports and Global Proliferation

Surveillance technology has become a global export commodity. China has sold AI and facial recognition software to Ecuadorian, Bolivian, and Peruvian authorities to enhance public surveillance, and has plans to construct networks of "smart" or "safe" cities in countries such as Pakistan and Kenya, with extensive monitoring technology built directly into their infrastructure

This export problem is not exclusive to China. Saudi Arabia serves as a striking example: Huawei is helping build safe cities, Google is establishing cloud servers, UK arms manufacturer BAE has sold mass surveillance systems, NEC is supplying facial recognition cameras, and both Amazon and Alibaba operate cloud computing centers in the country.

Threat 5: Generative AI and Information Operations

The malicious actors' use of AI tools and disinformation strategies enables the creation of convincing narratives that exploit individuals' biases, preferences, and vulnerabilities, making propaganda more effective and harder to detect. Evidence of this is already starting to emerge. A study by news monitoring service NewsGuard found that AI chatbots are spreading Russian misinformation and often failing to identify sources of disinformation.

Threat 6: Corporate Incentives Without Human Rights Oversight

Prior to pausing its Law-Enforcement Request Portal in June 2024, Amazon Ring had more than 1,300 partnerships with police departments across the U.S.

Freedom-of-information releases show Palantir's European public-sector contracts growing from tens of millions of euros in 2016 to hundreds of millions in 2024 — arrangements that conceal technical details behind trade-secret law, frustrating even well-resourced oversight committees.

Threat 7: Surveillance Gaps Within Liberal Democracies

Crucially, these threats are not confined to openly authoritarian regimes. The Snowden archive exposed NSA bulk-collection programmes such as PRISM, implemented without congressional awareness. The European Court of Human Rights later condemned UK bulk interception, yet the Investigatory Powers Act re-legalized data collection under closed "technical capability notices."

The legal standards required to legitimately carry out surveillance are high,

and even democracies with strong rule of law traditions and robust oversight institutions frequently fail to adequately protect individual rights in their surveillance programs.

5. Impact on International Peace and Security

The increasing number of AI-enabled surveillance systems has introduced challenges to international peace and security that extend well beyond their stated purposes of counterterrorism or public order. At the interstate level, the deployment of network-based surveillance tools against foreign officials creates a serious breach of diplomatic norms with direct security implications. The 2025 Israel-Iran conflict offered the most consequential illustration of this dynamic to date: Israeli intelligence, drawing on years of surveillance architecture built through signals intelligence and cyber spying, monitored nearly all traffic cameras in Tehran to conduct real time pattern of life analysis on senior Iranian officials, ultimately locating Supreme Leader Khamenei's whereabouts and enabling a targeted strike on his compound. This case demonstrates how surveillance infrastructure**,** when sufficiently advanced, collapses the distinction between intelligence gathering and lethal military action.

A particularly direct threat to international stability is transnational pressure, the practice by which governments extend their surveillance devices beyond their borders to monitor diaspora communities, political exiles, and foreign-based journalists. Iran's APT42 group, linked to the IRGC, has been documented monitoring Iranian journalists, activists, and academics abroad, as well as Western research institutions concerned with Iranian affairs. Freedom House has documented such operations managed by at least 38 governments across 91 countries, and AI-powered tools have significantly lowered the operational cost of these activities, enabling a government to monitor an opposition abroad without deploying a single human agent.

The competitive gaining of AI surveillance capabilities has further produced dynamics that parallel conventional arms races. As AI democratizes advanced cyber capabilities, the threshold for conducting effective asymmetric surveillance and warfare continues to lower, enabling smaller states and non-state actors to project power far beyond their traditional means. The Iran-Israel conflict illustrated this asymmetry clearly: while Israel concentrated cyber and surveillance power against hard state-controlled structures to benefit vulnerability, Iran harnessed mass surveillance through compromised civilian security cameras and automated phishing campaigns, achieving strategic psychological impact through volume rather than technical advancement.

Finally, the existing UN framework offers limited recourse for affected states. As Israel's National Directorate of Cyber noted, cyberattacks against the country increased by 55% in 2025 alone, with 26,000 incidents handled in a single year, a volume that existing versatile mechanisms are entirely unequipped to address. The Group of Governmental Experts on Information and Telecommunications Security has established voluntary norms for responsible state behavior in cyberspace, but these remain non-binding and their application to AI-specific surveillance tools is actively contested. The relationship between government sponsored surveillance and international peace and security therefore represents a present and structurally significant challenge requiring coordinated multilateral response.

6. Humanitarian and Human Rights Concerns

The deployment of AI-enabled surveillance systems by state actors raises concerns that cut across multiple internationally recognized human rights, including the right to privacy, freedom of expression, freedom of assembly, and the right to non-discrimination. Governments are increasingly deploying AI in areas such as surveillance, predictive law enforcement, biometric identification, behavioural profiling, and automated threat detection technologies that, even when pursued in service of legal security objectives, carry the potential to generate novel and unexpected violations of human rights and the rule of law. The Office of the United Nations High Commissioner for Human Rights has responded to this trend by calling for a moratorium on the sale and use of AI surveillance systems that pose serious risks to human rights until enough safeguards are in place, and has called for an outright ban on applications that cannot be made compliant with international human rights law.

The most foundational concern is the violation of the right to privacy, mentioned in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. AI-powered biometric systems reduce anonymity, limit individual autonomy, and potentially infringe upon the right to privacy, as well as freedoms of peaceful assembly, association, expression, and political participation. Beyond direct violations, mass surveillance produces what legal scholars term a “chilling effect”: the documented tendency of individuals to self-censor, withdraw from civic life, and avoid lawful association when they believe they are being observed. The UN Special Rapporteur on the rights to freedom of peaceful assembly and association has emphasized that AI-assisted surveillance not only leads to direct violations against affected individuals, but deeply undermines the ability to exercise fundamental freedoms and worsens chilling effects on political and democratic participation.

A structurally significant concern is the role of algorithmic bias in replicating and upgrading pre-existing patterns of discrimination. Predictive policing systems which claim to forecast criminal activity based on historical data are especially sensitive to this phenomenon. Amnesty International’s 2025 report stated that predictive policing systems encourage racist and discriminatory policing and the criminalization of areas, groups, and individuals continue institutional racism in policing and wider society. Because these systems are trained on historical law enforcement data that reflects decades of discriminatory practice, their outputs systematically disadvantage minority, low-income, and politically differentiated communities not as a malfunction, but as a natural consequence of their design. The UN Special Rapporteur on current forms of racism has further highlighted that AI-driven predictive models used in immigration surveillance are prone to creating and reproducing racially discriminatory feedback loops.

Facial recognition technology presents a particular challenge to the protection of human rights in public space. The American Civil Liberties Union has argued that face recognition technology makes it dangerously easy to identify and track

individuals at protests, political rallies, religious gatherings, and other constitutionally protected activities. At the international level, the same technology has been deployed by authoritarian governments as an instrument of political control. In Xinjiang, China, facial recognition systems integrated with behavioral scoring infrastructure have been used to monitor the Uyghur population with a comprehensiveness that human rights organizations have described as creating crimes against humanity. The Freedom Online Coalition's 2025 Joint Statement on AI and Human Rights noted that AI systems are now used systematically to suppress the opposition, manipulate public discourse, and reinforce inequalities trends that are becoming embedded in governance and law enforcement systems with fewer checks, less transparency, and greater cross-border impact.

A defining feature of the current landscape is the near-total absence of effective accountability mechanisms for those subjected to harm by state surveillance systems. The UN Special Rapporteur has emphasized that the threats posed by AI surveillance are made worse by the overall lack of transparency in how such technology is distributed, and the absence of proper regulation and meaningful oversight. Individuals who are misidentified, wrongfully marked, or placed under surveillance on the basis of incorrect algorithmic outputs often have no practical means of challenging those decisions, identifying their source, or acquiring redress. Many AI technologies are not simply dual-use but naturally repurposable applications developed for law enforcement and border control raise particular concerns about due process and the absence of accountability regarding states' commitments to human rights norms explained in the Universal Declaration of Human Rights. In the absence of binding international standards governing transparency, human rights impact assessments, and independent oversight, the gap between the impressive commitment of states to human rights and the operational reality of their surveillance practices continues to widen.

7. The Role of AI Bias in State Operations
8. International Legal Frameworks and Deals

The governance of AI-enabled surveillance at the international level is defined by a fundamental gap: technological development has consistently outpassed the capacity of legal institutions to respond. The foundational basis for regulating state surveillance derives from the International Covenant on Civil and Political Rights, whose Article 17 prohibits optional interference with privacy, a provision confirmed to apply to digital communications. While the UN General Assembly has reinforced this principle through successive resolutions calling on states to align surveillance practices with human rights obligations, none of these instruments introduced binding enforcement mechanisms specific to AI surveillance systems.

The most significant recent development is the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, adopted in May 2024 the world's first binding treaty on AI. It mandates risk assessments, establishes principles of transparency and accountability, and provides individuals the right to challenge AI-driven decisions. However, it carries a critical structural limitation directly

relevant to this committee: it explicitly excludes national security and defense activities from its scope, meaning the very category of government-sponsored surveillance most at issue falls outside its protections.

At the multilateral level, the Global Digital Compact, adopted at the UN Summit of the Future in September 2024, commits member states to ensure surveillance-related laws comply with international law and establishes an independent scientific panel on AI governance. The EU AI Act, also adopted in 2024, represents the most detailed regulatory model currently in existence, going as far as banning biometric mass surveillance within EU judgement though its reach is limited to member states and cannot bind third-country governments engaged in the operations this committee analyzes.

Taken together, the existing legal architecture presents three critical gaps. First, no binding multilateral instrument specifically governs AI in government-sponsored surveillance operations. Second, the only binding AI treaty openly disagrees to include national security activities. Third, even where frameworks exist on paper, the absence of transparency and meaningful oversight mechanisms makes enforcement possible against state actors largely aspirational. It is this governance vacuum that makes the present agenda item an urgent matter for multilateral arguments.

9. Positions of Key Member States

🇨🇳 China, People's Republic of

The most advanced user of AI state surveillance in the world is China . It operates under the doctrine of cyber sovereignty . Surveillance systems in Xinjiang and Tibet have been described as “Orwellian,” including mandatory DNA samples, Wi-Fi monitoring and facial recognition cameras connected to integrated data analysis platforms. Through its Digital Silk Road, China exports this model around the world. China will invoke sovereignty to defend its surveillance as an internal matter in committee, obstruct any binding accountability mechanism, and present its technology exports as development assistance.

Russian Federation (Russia)

Russia’s stance resembles China’s sovereignty-first approach, considering Western-led governance as hegemonic control. Russia’s UN delegate has said that AI systems “must be built on the cultural and national specifics of each civilization” and opposes external rule-setting by Western powers.Russia regularly uses the NSA/PRISM programs to expose the West’s hypocrisy. Russia will sit close to China in the committee room and undermine the moral authority of the Western delegations whenever it can.

United States of America 🇺🇸

The U.S. champions rights-based AI governance on the world stage but has credibility

gaps at home — The United States was the leader on the landmark March 2024 UN General Assembly resolution on “safe, secure and trustworthy” AI, co-sponsored by over 120 member states. But programs like PRISM and shifting attitudes to commercial spyware deeply erode its moral authority. In committee, the U.S. will advocate for human rights norms and export controls on surveillance tech, and resist any binding framework that would limit its own intelligence activities.

🇪🇺 EU

The EU offers the most advanced binding AI surveillance regulatory framework in the world. The EU AI Act, adopted in March 2024, prohibits social scoring, emotion recognition in the workplace, and biometric categorization systems in public spaces. The EU champions this model energetically as a global norm. In committee, EU member states will advocate for binding international frameworks and will cite the AI Act as an example for the world to follow.

🇬🇧 UK

The UK held the first global AI Safety Summit at Bletchley Park in 2023 and presents itself as a neutral convener of AI safety dialogue. The European Court of Human Rights, however, condemned bulk data interception by the UK but the Investigatory Powers Act again legalized the gathering of data through ‘technical capability notices’ which are closed. In committee, the UK will support transparency norms but resist firm treaty obligations on national security surveillance.

🇮🇳 India.

India claims to be an innovation-first AI leader, but one of the least regulated deployments of surveillance in the world. By 2024, there were more than 120 government facial recognition contracts recorded, with AI surveillance being deployed at airports, exam halls and public events. Despite well-documented risks, the government has said it will not intervene in the first wave of global AI regulations. In committee India will argue for a light touch on governance and against the imposition of binding limits on surveillance.

🇧🇷 Brasil

Brazil has emerged as the loudest voice from the Global South on AI governance, with the passage of the Brazilian AI Bill in 2024 and a $4 billion sovereign AI investment plan. Brazil is one of the countries developing strong data protection frameworks specifically to reduce surveillance and privacy violations. Brazil will chair the G20 and BRICS in 2025, and will use both platforms to bring AI governance to the multilateral agenda. Brazil will push for inclusive governance, capacity building and strong norms for data protection in the committee.

🇮🇱 **Israel**

Israel is a leading global exporter of surveillance technology, home to NSO Group — the developer of Pegasus spyware. Israel uses Pegasus licenses as diplomatic currency, approving sales to countries it wants something from, while the leaked Pegasus database contained 50,000 phone numbers across Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, and the UAE. Israel excels in world-class cybersecurity and defense AI capabilities. **In committee, Israel will resist export restrictions on surveillance**

technology and frame its tools as legitimate counterterrorism instruments.

🇦🇪 United Arab Emirates

The UAE has positioned itself as a major AI investor and smart city pioneer while maintaining one of the region's most extensive surveillance infrastructures. The UAE's AI company G42 has been scrutinized by U.S. Congress for ties to surveillance and spyware technology firms, and the Emirati government has a documented history of deploying mass monitoring tools against human rights defenders. **In committee, the UAE will oppose binding surveillance restrictions and favor light, industry-led regulation.**

🇸🇦 Saudi Arabia

Saudi Arabia is a documented user of both domestic and extraterritorial AI surveillance. The Saudi Crown Prince personally sought to restore Pegasus access after it was revoked following the Khashoggi assassination, and Khashoggi's fiancée's phone was infected just four days after his murder. Saudi Arabia simultaneously sources surveillance technology from Huawei, Google, BAE Systems, NEC, Amazon, and Alibaba. **In committee, Saudi Arabia will defend surveillance as a national security necessity and resist any binding accountability mechanism.**

🇰🇵 North Korea

North Korea operates the most closed and opaque domestic surveillance state in the world, with virtually no external accountability. North Korean cyber actors continue to improve their tactics and are now implementing AI to automate phishing attacks and cyberoperations. North Korea does not engage constructively in multilateral AI governance forums and primarily uses cyber capabilities for financial theft and regime survival. **In committee, North Korea will be largely obstructionist, rejecting any framework that implies external monitoring of state activities.**

🇮🇷 Iran

Iran uses AI-powered surveillance primarily to suppress domestic dissent and monitor opposition figures abroad. Iran is developing AI solutions mostly for its defense sector amid international sanctions. Iran has been documented using digital tools to target journalists, activists, and dissidents beyond its borders. **In committee, Iran will oppose any binding framework, align with Russia and China on sovereignty arguments, and reject Western-led governance initiatives as politically motivated.**

🇯🇵 Japan

Japan has adopted a cautious, comprehensive approach to AI governance, emphasizing safety and human rights without aggressive domestic surveillance deployment. Japan has adopted a more cautious regulatory approach, emphasizing comprehensive rules to mitigate risks rather than prioritizing innovation-first deregulation. Japan co-hosted the AI Safety Summit follow-up in Seoul in 2024 and actively participates in multilateral AI safety forums. **In committee, Japan will support balanced international frameworks combining innovation with strong human rights safeguards.**

🇰🇷 South Korea

South Korea occupies a unique position as both a major AI technology power and a victim of AI-enabled surveillance threats from North Korea. South Korea adopted the UN resolution on safe, secure and trustworthy AI in March 2024, and announced the "Seoul Declaration for Safe, Innovative, and Inclusive AI" during the AI Seoul Summit in May 2024. South Korea also passed its own AI Basic Act in 2024. **In committee, South Korea will strongly support multilateral AI safety frameworks and push for accountability mechanisms, particularly regarding state-sponsored cyber operations.**

🇩🇪 Germany / 🇫🇷 France

As leading EU member states, Germany and France broadly align with the EU AI Act framework but have at times pushed back against provisions they feared would stifle innovation. Both countries had misgivings about placing foundation models in the AI Act's high-risk category, reflecting tension between regulatory ambition and economic competitiveness. France co-hosted the 2025 AI Action Summit in Paris. **In committee, both countries will support binding surveillance restrictions within the EU model while seeking balanced treatment of dual-use AI technologies.**

🇹🇷 Turkey

Turkey sits at a complex crossroads — a NATO member with democratic institutions that has nonetheless expanded government surveillance significantly. Turkey has published multiple AI guidelines and has a bill for AI regulation in the legislative process, but human rights organizations have documented its use of digital surveillance against journalists and opposition figures. **In committee, Turkey will likely support sovereignty-based arguments on surveillance while nominally endorsing human rights language, navigating between its Western alliances and authoritarian tendencies.**

🇿🇦 South Africa

South Africa leads African AI governance efforts and has adopted an EU-influenced National AI Policy Framework. South Africa has adopted EU-like regulations through its National AI Policy Framework, addressing responsible AI development amid research capacity challenges. As a BRICS member, South Africa also advocates for South-South cooperation and greater Global South representation in international AI governance bodies. **In committee, South Africa will push for inclusive, human rights-aligned frameworks and demand equitable capacity-building for developing nations.**

🇳🇬 Nigeria / African Union

Nigeria, as Africa's most populous nation, represents the continent's concern about becoming a destination for unregulated surveillance technology exports. A breakdown of military expenditures shows that surveillance technology deployment correlates heavily with military spending, spanning from full democracies to authoritarian regimes. The African Union's Continental AI Strategy calls for inclusive international mechanisms where developing countries are equal participants in governance. **In committee, Nigeria and the AU bloc will demand binding export controls on surveillance technology and meaningful inclusion in global standard-setting.**

🇸🇬 Singapore

Singapore is a small but highly influential AI governance actor, combining advanced

technological deployment with relatively strong rule-of-law institutions. Countries such as Singapore prioritize business innovation and economic growth through light regulation and industry-led initiatives. Singapore has developed its own Model AI Governance Framework and positions itself as a bridge between East and West in multilateral negotiations. **In committee, Singapore will advocate for flexible, risk-based governance frameworks and oppose overly prescriptive binding restrictions.**

🇦🇷 Argentina / Latin America

Argentina represents the Latin American bloc's growing unease with both Chinese surveillance technology exports and Western-dominated governance frameworks. Argentina's dissociation from parts of the Global Digital Compact reflects wide unease in the Global South about frameworks perceived as encroaching on national autonomy. Latin American states are increasingly developing their own data protection laws. **In committee, Argentina and the Latin American bloc will push for sovereign, regionally appropriate governance solutions and resist both Chinese technology dependency and Western regulatory imposition.**

10. Questions to be Answered

1. How can governments use AI surveillance systems for security without violating human rights and personal privacy?
2. Should there be an international law or treaty regulating AI-powered surveillance technologies? If yes, what should it include?
3. How can the United Nations prevent the misuse of facial recognition and biometric identification systems?
4. To what extent should governments be allowed to monitor online activity and social media platforms for national security purposes?
5. How can the international community reduce algorithmic bias and discrimination in AI surveillance systems?
6. Should countries place export controls on surveillance technologies sold to authoritarian governments? Why or why not?
7. What measures can be taken to protect journalists, activists, exiles, and diaspora communities from transnational digital surveillance?
8. How can transparency and accountability be ensured when governments use AI in law enforcement and intelligence operations?
9. What role should private technology companies play in preventing human rights abuses linked to AI surveillance tools?
10. How can states cooperate internationally to address cyber threats, AI-driven misinformation, and digital authoritarianism while still respecting national sovereignty?