

BMUNIS'25 BACKGROUND GUIDE



UNITED NATIONS OFFICE ON DRUGS AND CRIME

LETTER FROM CHAIRS

Greetings Delegates,

We, Priyachitha K.K and Sreehari Suresh, the chairs of UNODC for BMUNIS'25 are extremely ecstatic to welcome you to a chamber of a governing body within the United Nations, where global threats involving cybercrime, drug trafficking and various other forms of crime shall be discussed, negotiated, and debated on.

Here, the future of global justice and security rests in your hands. As chairs of this thrilling council, it's our duty to guide you all through the dynamics of intense debates, negotiations and resolutions, that will keep you engaged and inspired- it is the United Nations Office on Drugs and Crime, after all!

This council is more than just a conference; it's a pivotal platform where decisions resonate throughout the world and shape the future. We encourage you to come well-prepared, as we will address critical issues that demand your attention and intellect.

To assist in your preparations, we have compiled a concise guide detailing the agendas for our discussions. While this guide is a valuable starting point, we emphasize the importance of conducting further research. Your preparation should reflect not only your country's stance but also the perspectives of your fellow delegates, fostering a richer dialogue.

We wish you the utmost success and look forward to an extraordinary conference filled with insightful contributions and collaborative spirit!

Please feel free to contact either one of us if you've got any doubts or questions you'd like to ask us!

With best regards,
Priyachitha K.K. & Sreehari Suresh

Chairpersons,

UNODC, BMUNIS'25

Priyachitha +973 3616 4886

Sreehari +973 3617 0617

ISSUE 1: SHOULD GOVERNMENTS SURVEILLANCE TO FIGHT CYBERCRIME OR DOES THIS INFRINGE ON PRIVACY AND HUMAN RIGHTS?

INTRODUCTION

Today's governments under tremendous pressure to increase public surveillance to curb cybercrime, which includes anything from crypto ware to online child exploitation. Proponents argue that to effectively identify, discourage, and investigate these emerging concerns, the state must increase its surveillance and data access. However, surveillance poses serious privacy and civil rights issues, especially when it is used extensively. Whether monitoring can be both efficient and respectful of individuals' rights is the true question.

The world is feeling the strain. Despite worries about cybersecurity and privacy, a new EU CSAM (child sexual abuse material) guideline would mandate that every digital correspondence be reviewed and scanned, endangering encryption and perhaps permitting widespread monitoring. The UN Cybercrime Convention, which comes into effect in late 2024, may, however, let countries to start restricting their capacity to collect data without stringent laws and limitations, especially in less democratic contexts, Human Rights Watch has warned. According to human rights frameworks, surveillance and monitoring must meet the requirements of legality, necessity, proportionality, and oversight. International Guidelines for Applying Human Rights to Communications According to surveillance, surveillance must be expressly permitted by law, have a valid

According to human rights frameworks, surveillance and monitoring must meet the requirements of legality, necessity, proportionality, and oversight. International Guidelines for Applying Human Rights to Communications According to surveillance, a legitimate objective, need, proportionality, and explicit legal authorization are all required, as are safeguards for the scope and use of monitoring. These prioritize the elimination of superfluous data, restricted involvement, and court power and monitoring—all of which are consistent with the Necessary and Proportionate Principles.

Furthermore, the use of monitoring often has horrible outcomes, like people self-censoring, journalists being unwilling to investigate, activists losing hope, and public discourse collapsing, all of which compromise democratic

participation and freedom of expression. Face recognition is one example of a biased technology that may amplify stereotypes and worsen systemic injustices.

Surveillance isn't always negative, though. Clear, regulated, rights-compliant, time-limited, targeted, and court-approved surveillance can help law enforcement better prevent cyberattacks. The UNODC aims to defend human rights while promoting technical efficiency and cooperation.

KEY TERMS AND CONCEPTS

- **Cybercrime:** The term is used to describe criminal activity using computers or the internet, including identity theft, hacking, cyberterrorism, online child manipulation, and crypto ware assaults.
- **Surveillance:** It is the surveying of behavior, mannerisms, activities, or information, is a popular tool used by governments and security organizations to gather information, influence, or control people or groups.
- **Mass Surveillance:** Mass surveillance is producing privacy and civil rights difficulties, is the indiscriminate collection of data on a wide variety of topics, often without exclusive skepticism.
- **Targeted surveillance:** Targeted surveillance is the practice of observing people or groups based on evidence or suspicion, typically with the consent of the court or other legal processes.
- **Privacy:** According to the United Nations Declaration of Human Rights and the International Covenant on Human and Political Rights, it is a fundamental human right that refers to the absence of coercive interference.
- **Encryption:** The process of turning data into a code to prevent unauthorized access is known as encryption. Digital communication is often protected by end-to-end encryption.
- **Chilling Effect:** The chilling effect is the result of someone avoiding proper words, actions, or behaviors because they are afraid of being noticed or facing legal repercussions.

- **Proportionality and Necessity:** According to these rules, all monitoring techniques must be suitable for the intended use and not overly broad.
- **The United Nations Cybercrime Convention (2024):** It is a global agreement aimed at preventing cybercrime anywhere in the globe. However, it has come under scrutiny for possibly allowing governments extensive monitoring capabilities without effective protections.
- **Metadata:** The time, date, sender, and recipient are examples of metadata, which is information regarding additional details that are not included in the communication's actual content. Governments often gather metadata for surveillance purposes that might possibly expose sensitive and private information.
- **Legal Interception:** It is frequently permitted by law for government officials to lawfully obtain private communications, including emails and phone calls.
- **Cybersecurity:** It is the process of defending computer systems, networks, and data from internet attacks. often used as a defense or argument in favor of surveillance.

GENERAL OVERVIEW

1. **What the Problem Is** In order to combat cybercrime, governments are increasingly adopting digital surveillance to monitor communications, gather information, take use of backdoors, and use hacking tactics.

2. **Historical Background & Inception** America the 1978 Foreign Intelligence Surveillance Act (FISA) created the Foreign Intelligence Surveillance Court and a warrant-based framework for monitoring foreign intelligence operations. After 9/11 and Snowden FISA amendments, particularly Section 702, expanded monitoring to cover non-Americans and communications that enter the country illegally. These capabilities are controversial because they blur the lines between domestic surveillance, even if they were reaffirmed. Edward Snowden's 2013 revelation of the PRISM program, which gave the government access to the servers of major corporations, sparked a global debate over state authority and privacy. United Kingdom Known as the "Snoopers' Charter," the Investigatory Powers Act of 2016 gave broad monitoring authority but was challenged in court. The foundation for the agencies that intercept and carry out surveys was already established by RIPA (2000). The Karma Police, a GCHQ mass-surveillance operation that

collected IP data without supervision, was also made public by the Snowden disclosures.

Proposals like the Communications Capabilities Development Programme (2010–13) were delayed due to legal issues, although they did influence later legislation.

3. Present Situation Environment of Cybercrime Worldwide by 2025, cybercrime is expected to cost the world economy roughly USD 10 trillion, and by 2029, it might cost USD 16 trillion. Ransomware, phishing, and credential theft are still major threats; in Q3 2024, ransomware impacted 1,275 businesses. Highlights by Region • In 2023, cyber-enabled fraud caused damages in Southeast Asia ranging from USD 18 to USD 37 billion. Initiatives like Serengeti show promise through international collaboration, but more than 75% of African nations lack adequate legislative or technical frameworks to handle cybercrime. Technological Trends.

4. The first artificial intelligence-generated malware appeared in early 2025. Two of the most challenging places to secure are public cloud settings and mobile devices.

5. UNODC's Global Response The UN Cybercrime Convention (2024) offers a legal framework that safeguards human rights, promotes collaboration, and aids nations with low financial resources. National Projects • The overall amount of money lost increased from USD 8.5 million to USD 25 million, and the number of Uzbek teenagers who fell victim to cybercrime increased from 20,000 to over 30,000 between 2022 and 2023. UNODC is helping with digital literacy and legal reforms. 4. Summary: Completed Steps The Investigatory Authorities Act (UK) and FISA (US) are two statutes that specify surveillance authorities. Disclosures like the Snowden revelations spark controversy and legal opposition. A global accord that balances law enforcement and rights is being drafted by the UNODC. One regional project that is building capability is Uzbekistan.

6. Subjects of Persistent Importance North America and Europe are crucial areas for surveillance activities and policy discussions. Southeast Asia and Africa are hotspots for cybercrime because of their increasing internet adoption and poor infrastructure. The UN Cybercrime Convention seeks to encourage a human rights- abiding, cooperative response.

MAJOR PARTIES INVOLVED

UNITED STATES

The US leads the world in cyber capabilities and surveillance infrastructure. Thanks to laws like the Foreign Intelligence Surveillance Act (FISA), particularly Section 702, and systems like PRISM, foreign nationals can be closely watched. Despite criticism for extensive surveillance and potential violations of human rights, the US backs strong cybercrime enforcement.

UNITED KINGDOM

The United Kingdom has one of the most advanced surveillance systems in the world. The Investigatory Powers Act of 2016 (also known as the "Snoopers' Charter") legalizes widespread data collection, metadata retention, and government hacking. The Snowden files contain revelations on widespread surveillance that have been connected to UK intelligence services such as GCHQ.

RUSSIA

To quell opposition and criminality, Russia advocates for a state-run internet (the "sovereign internet") and robust monitoring capabilities. It rejects legally binding human rights clauses in treaties yet supporting international cooperation on cybercrime. It has also been accused of conducting state-sponsored cyberattacks.

CHINA

Real-time facial recognition, internet monitoring, and censorship are all part of one of the world's largest digital surveillance networks in China. It makes the case that maintaining national security and reducing crime depend on its technique. It opposes Western privacy laws and supports the idea of "cyber sovereignty".

EUROPEAN UNION (EU MEMBER STATES)

The General Data Protection Regulation (GDPR) is one of the main ways that the EU promotes human rights and data protection. Member nations vary, nevertheless, in their methods of surveillance. The EU backs the UN Cybercrime Convention but insists on human rights and surveillance protections.

INDIA

With laws like the Information Technology Act and pending legislation like the Digital Personal Data Protection Act, India has increased its surveillance capabilities in response to the country's rising cybercrime issue. Its surveillance system is criticized for lacking judicial supervision and openness.

BRAZIL

Brazil has a say in discussions on internet governance worldwide. In addition to fighting cybercrime, particularly financial fraud, it advocates for robust privacy rights (e.g. Marco Civil da Internet). Brazil actively engages in discussions for a UNODC cybercrime pact, highlighting the need to strike a balance between human rights and enforcement.

SOUTH AFRICA

South Africa, a leading voice of Africa, is in favor of more international collaboration on surveillance and cybercrime. Additionally, it promotes making sure that all surveillance practices uphold access to justice and constitutional rights.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC)

Oversees drafting and promoting the UN Cybercrime Convention to establish a worldwide legal framework for combating cybercrime. It strikes a balance between human rights safeguards and law enforcement operations.

INTERNATIONAL TELECOMMUNICATION UNION (ITU)

Encourages the growth of global cybersecurity capabilities and standards, particularly in emerging nations. It is essential to internet governance and digital infrastructure.

COUNCIL OF EUROPE

It oversees the first international agreement against cybercrime, the Budapest Pact on Cybercrime (2001). Russia and China oppose it, while the US, EU, and others favor it.

INTERPOL

Coordinates information exchange and international law enforcement activities related to cybercrime. To enhance international response, it

implements initiatives like the Cybercrime Directorate and public-private collaborations.

EUROPEAN UNION (EU)

The EU facilitates cybersecurity collaboration among its member states through organizations like Europol and ENISA. Additionally, it advocates for global accords that conform to European privacy norms.

TIMELINE OF MAJOR EVENTS

1948 — Universal Declaration of Human Rights. Article 12 establishes the right to privacy: "No one shall be subjected to arbitrary interference with his privacy..." This becomes a worldwide standard referenced in all surveillance-related human rights debates.

1978 — U.S. Foreign Intelligence Surveillance Act (FISA) passed. Establishes legal framework for electronic surveillance in the U.S. Creates the secret FISA Court to authorize spying on foreign agents.

2001 — USA PATRIOT Act Enacted (U.S.) After 9/11, U.S. significantly develops surveillance powers. Section 215 enables mass metadata collection (e.g. phone records).

TIMELINE OF NOTABLE EVENTS

1948 — Universal Declaration of Human Rights. Article 12 safeguards the right of privacy: "No one shall be subjected to arbitrary interference with his privacy." Becomes the international norm cited in every contention involving surveillance and human rights.

1978 — U.S. Foreign Intelligence Surveillance Act Passed. Codifies U.S. law regarding electronic surveillance. Creates the FISA secret court to approve spying on foreign spies.

2001 — USA PATRIOT Act Enacted (U.S.). U.S. greatly increases surveillance authority after 9/11. Section 215 permits bulk collection of phone records (metadata).

2001 — Budapest Convention on Cybercrime Adopted. First international treaty dedicated solely to cybercrime. Signed by Council of Europe and members, including U.S. (but not by China, India, nor Russia). Encourages global cooperation but criticized as weak on privacy protections.

2013 — Snowden Leaks. Former NSA employee Edward Snowden releases private data to the public. reveals mass surveillance programs like as

Tempora, XKeyscore, and PRISM generates debate and agitation about privacy and national security issues globally.

2016 — The UK Investigatory Powers Act was put into effect. Justifies the bulk collection and bulk surveillance by UK agencies. Strongly criticized by privacy groups; also called the "Snoopers' Charter".

2018—EU General Data Protection Regulation (GDPR) Adopted. Imposes strict privacy and data protection regulations across the EU. Requires the gathering of data with express consent and provides individuals with rights to their information.

2020 — COVID-19 Digital Contact Tracing. The governments widely use location tracking and surveillance extensively to track the movement of the coronavirus. Raises fear of temporary surveillance becoming permanent.

2021-2024 — Negot's UN Cybercrime Convention. An international treaty on cybercrime has been suggested by the UNODC. Negotiations expose deep divisions: Western democracies work to protect private information and respect human rights. Russia, China, and their many allies are in favor of government regulation of the internet.

2023 — Congress is considering reforming FISA. fierce political battle to renew or change Section 702. Civil rights organizations are calling for more privacy protections.

2024 — Adoption of the UN Cybercrime Convention. Adopted by majority vote of the UN General Assembly. Calls for harmonization of laws and increased cooperation citing human rights. Critics argue that it omits robust enforcement of privacy protections.

2025 — Surveillance & Cyber-Assisted Artificial-Intelligence. Both governments and cybercriminals utilize AI. First publicized cases of AI-authored ransomware appear. Surveillance technology is constantly evolving, raising further controversy globally on the issue of privacy

PREVIOUS ATTEMPTS MADE TO RESOLVE THIS ISSUE -

UNITED STATES

The United States has led the controversy regarding surveillance since the Snowden leaks in 2013. In 2024 President Biden signed into law a measure reauthorizing Section 702 of the Foreign Intelligence Surveillance Act, which potentially allows warrantless collection of information on foreign nationals.

Civil-rights groups demanded greater protection, but critical reforms such as requiring a warrant before getting hold of Americans' data were left out. Privacy and Civil Liberties Oversight Board suggested further judicial review and greater openness, thereby the dialogue in Congress persisted. Bills like the Government Surveillance Reform Act and the Fourth Amendment Is Not for Sale Act sought to limit warrantless access and stifle data broker spying, but they were opposed. Those attempts appear to have led to debate about reform, yet change remained limited, most probably because of lobbying and party division.

UNITED KINGDOM

The United Kingdom passed the Investigatory Powers Act 2016, legislating for sweeping surveillance, including metadata gathering, state hacking. To hold power in check, the government set up the Investigatory Powers Commissioner's Office, which monitors warrants and scrutinizes actions.

The law does have some judicial oversight and some transparency, but privacy organizations argue that it allows bulk surveillance without oversight. The UK system is held up by many as the ideal example of strong oversight yet offers little protection for individual liberty.

INDIA

India built its surveillance system through law such as the IT Act, but only recently gained a comprehensive data-protection statute. NGOs like the Internet Freedom Foundation try to map the spread of such technologies as facial-recognition – they call it Project Panoptic – and offer legal help to journalists and activists. The Akancha Srivastava Foundation also conducts workshops and a helpline with the aim to generate digital-safety awareness. These efforts seem to raise public consciousness and certain legal pressure, but the government's disclosure of surveillance is still limited, so enforcement of rights online continues to be patchy.

EUROPEAN UNION

The EU values privacy because of the GDPR. It endorses the Budapest Convention and the UN Cybercrime Convention but only if private information is protected and surveillance mechanisms are regulated. The Clean IT Project, which is run by several member states, tried to come up with guidelines for tearing down illegal online content.

Because the approach is soft-law, public-private partnership is encouraged but so is the constraining impact of being voluntary. The EU may still be a pioneer in bringing in privacy into cybercrime policy, however. Does that

mean that privacy will be kept safe. New York City (USA) At the city level, New York passed the POST Act in 2020, requiring the NYPD to disclose what spying technology they use. An amendment in 2024 attempts to enhance transparency regarding third-party access and data-retention. The act was towards accountability but is decried as toothless in that it does little to decrease surveillance overkill.

AFRICAN UNION

African Union supported the Malabo Convention for African to create regional laws on cybercrime and personal data. Implementation is sometimes slow, as there are no legal frameworks in most countries. Ratification levels are low and funding falls short. The convention appears to be a steppingstone for digital rights on the whole continent. Critics argue without more support the goals may remain talk.

UNITED NATIONS

At the global really level UNODC pushed the UN Cybercrime Convention, adopted in 2024 after talks. The deal aims to create an international network for cooperation, but its efficacy might be doubted.

RUSSIA and **CHINA** seemed to favor higher state control, while the EU fought vigorously for human-rights safeguards. The language mentions privacy but does not have binding implementation, a faulted weak point. Therefore, the accord demonstrates just how challenging global accepted consensus is, but it represents a step in the direction of cyber laws harmonization.

POSSIBLE SOLUTIONS

STRICTER OVERSIGHT & JUDICIAL REVIEW:

Make all surveillance plans subject to approval by independent judges and undergo routine audits.

LEGISLATION FOR TRANSPARENCY:

Make governments report publicly on the deployment of surveillance technologies and information.

INTERNATIONAL CYBERCRIME COOPERATION WITH RIGHTS PROTECTIONS:

Encourage global treaties (like the UN Cybercrime Convention) that include strong human rights safeguards.

DATA PROTECTION LEGISLATION:

Pass strong data privacy legislation to limit misuse of data collected through surveillance.

ENCRYPTION SUPPORT:

Protect end-to-end encryption and ban mandatory backdoors in communications software

BIBLIOGRAPHY

- https://gomun.cz/wpcontent/uploads/2023/10/Study_Guide_UNODC.pdf
- https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act?utm_source=
- House votes to reapprove law allowing warrantless surveillance of US citizens | US politics | The Guardian
- Investigatory Powers Act 2016 - Wikipedia
- Karma Police (surveillance programme) - Wikipedia
- Regulation of Investigatory Powers Act 2000 - Wikipedia
- International Principles on the Application of Human Rights to Communications Surveillance - Wikipedia
- Government & Corporate Surveillance | eReader
- Surveillance and Human Rights | Electronic Frontier Foundation
- United Nations Convention against Cybercrime
- The EU wants to scan every message sent in Europe. Will that really make us safer? | Apostolis Fotiadis | The Guardian
- Human Rights and the Global Digital Surveillance Infrastructure
- Right To Privacy And The Expanding Scope Of Surveillance - IJLSSS
- [2010.07023] Understanding bias in facial recognition technologies
- Human Rights and Surveillance: A Critical Examination of Privacy - Legal Brainiac
- Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights Human Rights Watch
- United Nations Convention against Cybercrime
- The EU wants to scan every message sent in Europe. Will that really make us safer? | Apostolis Fotiadis | The Guardian
- Government & Corporate Surveillance | eReader
- Human Rights and the Global Digital Surveillance Infrastructure

- International Principles on the Application of Human Rights to Communications Surveillance - Wikipedia
- Data and Surveillance - Useful Definitions | Privacy International Metadata - Wikipedia
- Why Communication Metadata Matters | Surveillance Self-Defense Government hacking - Wikipedia
- Computer and network surveillance - Wikipedia Dataveillance - Wikipedia
- House votes to reapprove law allowing warrantless surveillance of US citizens | US politics | The Guardian
- Senate Passes Spying Bill, Rejecting Privacy Concerns - WSJ How the NSA nearly destroyed the internet | WIRED Investigatory Powers Act 2016 - Wikipedia
- Regulation of Investigatory Powers Act 2000 - Wikipedia History of mass surveillance in the United Kingdom - Wikipedia Cybercrime worldwide - statistics & facts | Statista
- Cybercrime worldwide - statistics & facts | Statista
- UNODC Report: Southeast Asia a Rising Hub for \$37 Billion Cybercrime Industry
- Cybercrime Surge in Africa: INTERPOL's 2025 Report Unveils Digital Crisis Across the Continent - UNDERCODE NEWS
- Cybercrime Statistics 2025: Rising AI Threats & Global Impact • SQ Magazine
- Timeline of global surveillance disclosures (2013–present) - Wikipedia
- UN General Assembly adopts milestone cybercrime treaty | The United Nations Office at Geneva
- United Nations treaty on cybercrime agreed by the Ad Hoc Committee - Cybercrime
- UN General Assembly adopts landmark convention on cybercrime | United Nations in Egypt
- Basic facts about the global cybercrime treaty | United Nations
- Welcoming Adoption of Historic Cybercrime Convention, Secretary-General Urges All States Join to Promote Safe Cyberspace | Meetings Coverage and Press Releases
- UN General Assembly adopts landmark convention on cybercrime | United Nations in Egypt
- INTERPOL welcomes adoption of UN convention against cybercrime Budapest Convention on Cybercrime - Wikipedia
- Commission proposes to sign and conclude the UN Convention against Cybercrime - European Commission

- [Between a Rock and a Hard Place: The UN Cybercrime Convention - PRIF BLOG](#)
- [Senate passes reauthorization of key US surveillance program | AP News](#)
- [Privacy and Civil Liberties Oversight Board Embraces Surveillance Reforms | Brennan Center for Justice](#)
- [Government Accountability And Data Privacy: Evolving Policies, Lawsuits, And Oversight - The BayNet](#)
- [Policy Recommendations | Freedom House](#)
- [Welcoming Adoption of Historic Cybercrime Convention, Secretary-General Urges All States Join to Promote Safe Cyberspace | Meetings Coverage and Press Releases](#)
- [Investigatory Powers Act 2016 - Wikipedia](#)
- [Internet Freedom Foundation - Internet Freedom Foundation](#)
- [Akancha Srivastava Foundation - Wikipedia](#)
- [A Roadmap for Organizations Fighting Digital Surveillance](#)

ISSUE 2- THE BORDER SECURITY VS HUMANITARIAN CRISIS

DILEMMA

INTRODUCTION

The conflict between border security and responding to humanitarian obligation has emerged as a controversial and complex global issue. Most countries are under mounting pressure to tighten their borders more closely as threats such as drug trafficking, people smuggling, terrorism, and illegal migration escalate. These threats have necessitated policies for surveillance, detention, and physical barriers to prevent unauthorized entry and cross-border crime. They affirm that such measures are needed to maintain national security and public order.

But these same policies tend to inflict great hardship on refugees, asylum seekers, and other vulnerable migrants fleeing war, persecution, or extreme poverty. Increased border controls can block access to asylum procedures, leave individuals stranded in dangerous transit zones, and fuel greater reliance on hazardous migration routes. In some cases, border tightness has even yielded human rights violations, including pushbacks, arbitrary detention, and family separation.

Such a choice raises an old question: are border policies about stopping illegal and injurious activity, or ensuring the rights and dignity of individuals in need of humanitarian protection? With civil strife, environmental disaster, and political unrest driving people out of their countries all over the world, governments are forced to weigh curbing their borders with upholding their international obligation to protect asylum seekers.

KEY TERMS AND CONCEPTS

BORDER SECURITY

Measures implemented by a state to manage and monitor the flow of people, goods, and services across its borders, primarily to prevent illegal activities like trafficking, smuggling, and terrorism.

ASYLUM SEEKER

A person who has fled their home country and is looking for refuge in a foreign country. Their refugee status has not been legally granted yet.

REFUGEE

A person who has had to leave their country because of war, persecution, or violence and has received protection under international law, like the 1951 Refugee Convention.

IRREGULAR MIGRATION

Movement of people that occurs outside the established rules of the origin, transit, or destination countries.

PUSHBACKS

Forcibly sending back migrants or asylum seekers at the border without assessing their need for protection. This is usually a violation of international law.

NON-REFOULEMENT

A rule of international refugee law that prohibits returning asylum seekers to a country where they might face danger or persecution.

EXTERNALIZATION OF BORDERS

Policies where states shift migration control to other countries, such as the EU funding North African countries to stop migration, often raise concerns about human rights.

HUMAN TRAFFICKING

Illegal trade in human beings for forced labor or sexual exploitation. This activity is typically organized across open or poorly regulated borders.

SMUGGLING OF MIGRANTS

The illegal entry of a person into a state, often for financial gain, typically involving the migrant's behalf.

DETENTION CENTERS

Places where migrants, refugees, or irregular immigrants are held while their immigration status is resolved. These centers often have questionable circumstances.

SAFE AND LEGAL PATHWAYS

Options like resettlement programs, humanitarian visas, or family reunifications that allow migrants to enter a state legally and safely.

MIGRATION GOVERNANCE

The groups, rules, and laws that manage the movement of people between countries and balance national interests with humanitarian needs.

SOVEREIGNTY

The right of a state to control its borders and decide who it permits to enter and remain on its land.

UNHCR (UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES)

The UN agency that protects and supports refugees and promotes their rights under international law.

HUMANITARIAN CORRIDORS

Routes that help safely evacuate civilians, especially refugees, from areas affected by conflict or disaster.

GENERAL OVERVIEW

The tension between safeguarding national boundaries and upholding humanitarian responsibilities has become a hallmark theme of modern world politics. Governments are increasingly using stringent border policies to combat illegal immigration, narcotics trafficking, human smuggling, terrorism, and trafficking, on the one hand. Secure border regulation is seen as the need for national sovereignty, public safety, and law enforcement, on the other hand.

But the very same policies can have disabling effects on vulnerable populations—refugees and asylum seekers—forced to flee violence, persecution, or political turmoil. Border walls, detention centers, pushbacks, and externalized border management (e.g., offshoring migration control to third states often close off legal routes to asylum procedures and violate international humanitarian law, including the non-refoulement principle.

The issue is especially urgent with global displacement reaching record highs—over 120 million forcibly displaced persons worldwide as of 2024 (UNHCR). Travel is driven by conflict, poverty, environmental degradation, and state persecution. Most refugees are forced to adopt irregular, risky routes, and many are aided by smugglers, vulnerable to exploitation, abuse, and violence along the way.

Attempts to alleviate this tension have existed in the shape of global legal agreements, such as the 1951 Refugee Convention, the Global Compact on Refugees, and regional accords like the EU's New Pact on Migration and Asylum. However, implementation is sporadic, and political resistance often limits humanitarian access.

Striking the balance between legitimate border management and protection of human rights remains a top priority. The solution must be equitable and sustainable in the form of expanding safe and regular migration flows, improving asylum processes, and encouraging accountability for border management—while addressing the root causes of forced displacement

MAJOR PARTIES INVOLVED

UNITED STATES

The US takes center stage about global migration policy, especially the southern border. Title 42 policies, border wall construction, and detention policy have all created controversy surrounding balancing security and humanitarian commitment. The US also engages in border security efforts elsewhere, such as Latin America and the Caribbean, and is a top donor to refugee agencies.

EUROPEAN UNION (EU)

The EU finds itself at the center of the controversy, especially from African and Middle Eastern migration paths. While the New Pact on Migration and Asylum will attempt to harmonize policy among member states, the EU has also outsourced border control—cooperating with states like Libya and Tunisia to stem migration, commonly by sacrificing the rights of refugees.

GREECE, ITALY, AND SPAIN

These EU border nations are faced with huge numbers of refugees and migrants pouring in through the Mediterranean. They've been vocal about needing more help from other members of the EU and have also been accused of pushbacks and inhumane treatment of refugees in camps.

TIMELINE OF KEY EVENTS

1948 — Universal Declaration of Human Rights adopted. It may be interpreted that anyone can seek protection when persecuted.

1951 — Refugee Convention adopted. It defines who might be a refugee and making them return is forbidden.

1989 — UN Convention on Children's Rights. It appears to incorporate protection for child refugees and asylum seekers.

1990s — More fences and walls were erected by nations. Additional chain-link segments were placed across the U.S-Mexico border.

2001 — Post-9/11 security shift toughened borders. States linked controls of migration with counter-terror interests.

2005 — EU implemented Schengen Information System. Police now share information on migrants and crime across Europe.

2015 — European refugee crisis peaks at over a million arrivals. Syrians, Afghans and Iraqis fueled hot debates around security vs. aid.

2016 — EU-Turkey migration deal signed. Turkey agreed to reducing flows for cash and political support, a move others call short-sighted.

2018 — UN adopted Global Compact on refugees. It attempts to share the burden but lacks firm enforcement.

2019 — Australia's off-shore detention policy continues. Distant island asylum seekers, an institution that doesn't ring true.

2020 — COVID-19 pandemic closes the doors. Public health excuses persist in limiting asylum, raising emergency rights concerns.

2023 — EU launches new migration pact. It seeks to balance restricted borders with minimum protection, but its remit is doubted by critics.

2024 — In a controversial scheme, the UK will deport Rwandan asylum applicants. Plan to send overseas for processing provokes legal fights.

2025 — Global displacement hits record high. UNHCR reports more than 122 million displaced individuals, with underlying crisis.

The world seems not to be able to achieve a balance between security, rights, and compassion for displaced individuals.

PAST ATTEMPTS TO SOLVE THE PROBLEM

Attempts to balance the conflict between border security and humanitarian protection have been diverse, including legal regimes, bilateral agreements, regional strategies, and humanitarian initiatives.

The 1951 Refugee Convention and 1967 Protocol are key international treaties that set standards for protecting refugees. One important part is the non-

refoulement principle, which stops countries from sending refugees back to unsafe situations. Although nearly every country accepts this principle, its application is not consistent. This leads to protection gaps among different states.

The Global Compact for Refugees. In 2018, the UN General Assembly endorsed the Global Compact on Refugees. This initiative aims to improve international cooperation, share responsibilities, and support refugees.

Although it has received global backing, its enforcement is limited. It is not legally binding and relies on voluntary commitments.

By blocking migrants from entering Europe, the 2016 EU-Turkey Deal aimed to reduce irregular migration to the European Union. The deal decreased arrivals but faced criticism for human rights issues in Turkish refugee centers and allegations of pushbacks. It had some success in securing the border, but it also raised humanitarian concerns.

The EU's 2023 New Pact on Migration and Asylum attempts to balance faster asylum processing, stronger border security, and increased resettlement. However, political disagreements among member states and differing national interests have made it hard to implement consistently.

Countries like Australia have taken a strict stance by using offshore detention centers to prevent asylum seekers from arriving by sea. While these actions have decreased the number of boat arrivals, human rights groups have criticized them for poor living conditions and violations of human rights, which has damaged their credibility.

The United States has shifted between strict enforcement policies, such as building border walls and separating families, and more compassionate strategies like Temporary Protected Status. Recent administrations have focused on border security while addressing legal and ethical issues related to the rights and due process of asylum seekers.

International organizations like UNHCR and IOM work to improve humanitarian aid, legal entry points, and state capacity. NGOs provide essential frontline relief and advocacy, but they often encounter access restrictions and lack of funding.

Overall, success is based on political will, cooperation from the international community, respect for human rights, and eradication of migration's root causes. Failure often results from securitization prevailing over protection, lack of burden-sharing, and ineffective legal avenues for migration and asylum.

POSSIBLE SOLUTIONS

- Expand the legal and safe channels. To reduce dangerous irregular migration, increase resettlement programs and humanitarian visas.
- Enhance Asylum Systems. Speed up and strengthen fair asylum processing to protect genuine refugees.
- Boost International Cooperation. Share responsibility among countries of origin, transit, and destination to manage migration more effectively.
- Safe Borders with Rights Monitoring. Use technology and trained personnel to secure borders while ensuring humanitarian oversight and legal protections.
- Correct Root Causes – Invest in ending conflict, poverty, and climate resilience in countries of origin to reduce forced migration.
- Assist NGOs and Host Countries – Involve civil society and local partners in providing aid and integration assistance.

BIBLIOGRAPHY

- Border Procedures in the European Union: How the Pact Ignored the Compacts
- The Border Harms of Human Displacement: Harsh Landscapes and Human Rights Violations
- Migration: Fundamental rights issues at land borders | European Union Agency for Fundamental Rights
- The Interplay of Sovereignty and Refugee Protection in International Law - World Jurisprudence
- Frontiers | Crisis Without Borders: What Does International Law Say About Border Closure in the Context of Covid-19?
- Non-refoulement - Wikipedia
- [2207.04480] Strategic Choices of Migrants and Smugglers in the Central Mediterranean Sea
- Border Management and Human Rights - Border Security Report
- Article: Migrants' Human Rights: From the Margins .. | migrationpolicy.org
- Externalization of Border Controls as a Violation of Human Rights of Irregular Migrant Children: A Global Dilemma
- Article: Migrants' Human Rights: From the Margins .. | migrationpolicy.org
- [2107.12080] Rohingya Refugee Crisis and the State of Insecurity in Bangladesh
- Externalization (migration) - Wikipedia

- [2410.17278] Automated decision-making and artificial intelligence at European borders and their risks for human rights
- Convention Relating to the Status of Refugees - Wikipedia Detention of refugee children in Thailand - Wikipedia
- Refugees, Asylum Seekers and Migrants - Amnesty International Non-refoulement - Wikipedia
- Note on Non-Refoulement (Submitted by the High Commissioner) | UNHCR
- Externalization (migration) - Wikipedia Humanitarian crisis - Wikipedia Refugee law - Wikipedia
- Refugee studies - Wikipedia
- UNHCR master glossary of terms | UNHCR Access to territory and non-refoulement | UNHCR
- [2410.17278] Automated decision-making and artificial intelligence at European borders and their risks for human rights
- Wars have now displaced over 122 million people as aid funding falls, UN says | Reuters
- UN refugee agency says more than 122 million people forcibly displaced worldwide | AP News
- The Global Compact on Refugees | UNHCR Global Compact on Refugees - Wikipedia
- Pact on Migration and Asylum - European Commission
- The Council adopts the EU's pact on migration and asylum - Concilium
- European Parliament approves migration and asylum pact after years of deadlock
- Why immigration is back on the European Union's agenda | European Union | The Guardian
- Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals | Congress.gov | Library of Congress
- The Council adopts the EU's pact on migration and asylum - Concilium Pact on Migration and Asylum - European Commission
- Syria Emergency | UNHCR Turkey
- Universal Declaration of Human Rights | United Nations
- The Council adopts the EU's pact on migration and asylum - Concilium
- The 1951 Refugee Convention and 1967 Protocol relating to the Status of Refugees | UNHCR
- Convention on the Rights of the Child | OHCHR EU-Turkey statement, 18 March 2016 - Concilium Europe | UNHCR