# HASMUN

ITU

TABLE of CONTENTS:

1. Letter From the Secretary-General

Dear Delegates,

Welcome to HASMUN 2025 — a journey that goes far beyond a typical Model United Nations conference.

This year, we invite you to become part of an experience built on diplomacy, dialogue, and the determination to create change. HASMUN has long stood as a platform for driven individuals to challenge perspectives, develop leadership, and speak for the world they envision. In every committee room, in every debate, we believe your voice has the power to shape not only resolutions, but real ideas for the future.

Whether this is your first MUN or one of many, we encourage you to approach each session with openness, curiosity, and commitment. The friendships you form, the ideas you exchange, and the challenges you overcome will stay with you long after the final gavel falls.

On behalf of the entire Secretariat, we are thrilled to have you with us. Prepare to question, to collaborate, and to grow.

We look forward to meeting you soon.

Warm regards,
Nazrin Sadigova
Secretary-General
HASMUN 2025

2. Letter From the Committee Board

Dear delegates,
Welcome to HASMUN'25 and ITU Committee!
We are İrem Ayber, Öykü Efendi and Bengs İlban, your committee board members and Selim Uraz Gedikli, your academic assistant. We are having the honor to serve as the board members of this committee.
On behalf of the Committee Board for the ITU Committee, we extend our warmest welcome to all delegates. We are thrilled to have you participate in this prestigious Model United Nations conference. The ITU Committee focuses on critical issues related to human rights, emphasizing the importance of combating deepfake and synthetic media. As delegates, you have a unique opportunity to engage in meaningful debate, negotiation, and problem-solving to address these pressing issues. This study guide contains many prominent information about the agenda while giving an open space for you to also do your own research. Remember, regardless of your country's position in the agenda, you are all equal in the committee and you have all the resources in your hands to come up with great solutions and innovative ideas to achieve the goals set by the committee. We wish you all the best in your preparations and look forward to seeing you at HASMUN'25.

Best regards,
İrem Ayber, Öykü Efendi, Bengs İlban, Selim Uraz Gedikli

3. Introduction to the Committee: International Telecommunication Union

The **International Telecommunication Union (ITU)** is a specialized agency of the United Nations for information and communication technologies. Being founded in 1865 as the International Telegraph Union, it is the oldest international organization that still continues its activities. The Union consists of 194 Member States of the United Nations, and nearly 900 active organs of the sector (governments, telecom companies, universities) from its base in Geneva Switzerland. Its core mission is to enhance global connectivity and promote universal access to digital technologies. The union's actions include allocating

radio spectrum and satellite orbits, enhancing technical standards for telecommunication networks.

ITU is mostly known for its Connect 2030 Agenda on ensuring global use and benefiting from digital information helping the advancement of the UN's Sustainable Development Goals.

- **1865**: Representatives of 20 countries signed the first International Telegraph Convention in Paris, creating the *International Telegraph Union* to standardize cross-border telegraphy, the exact date of 17 May 1865 is now celebrated as World Telecommunication and Information Society Day.
- **1932**: The Union was renamed as the *International Telecommunication Union* after an expansion in the Union's focus.
- **1947–1949**: Following the UN's foundation, ITU came to an agreement with the United Nations to become a UN specialized agency
- **1948:** ITU moved its headquarters from Bern to Geneva and joined other UN agencies in Switzerland

ITU's aim is to improve international telecommunication. It holds a unique place in the UN's bodies because of its preservation of both governments and actors of the private sector. ITU Member States meet every four years at the **Plenipotentiary Conference** to discuss future policies and elections.

ITU's works are divided into three sub-bodies focusing on different areas:

**Radiocommunication (ITU- R)**: This body manages the global use of radiocommunication. ITU- R organizes World Radiocommunication Conferences every 3-4 years to revise the radio spectrum allocations and provide equal, effective and sufficient use of services.

**Telecommunication Standardization (ITU- T):** This body develops international technical standards for global telecommunications. These standards are prepared by groups of the private sector and approved at the World Telecommunication Standardization Assembly. ITU- T's work ensures that networks and devices are effectively used around the world.

**Telecommunication Development (ITU- D)**: This body promotes affordable access to information and communication technologies in developing regions. ITU- D provides technical assistance, capacity building and legal advice to help countries expand connectivity. It also emphasises the importance of enhancing digital skills, emergency communications, cybersecurity capacity, and other development issues.

In all these roles, ITU's core responsibilities related to our agenda are to set standards and policies, and help extend information and communication technologies infrastructure. ITU's *Radiocommunication Bureau* publishes the *Radio Regulations Treaty*. Its Standardization Bureau maintains a database of recommendations for the states and private sector partners. The Development Bureau runs programs and publishes data to guide global information communication technologies' planning.

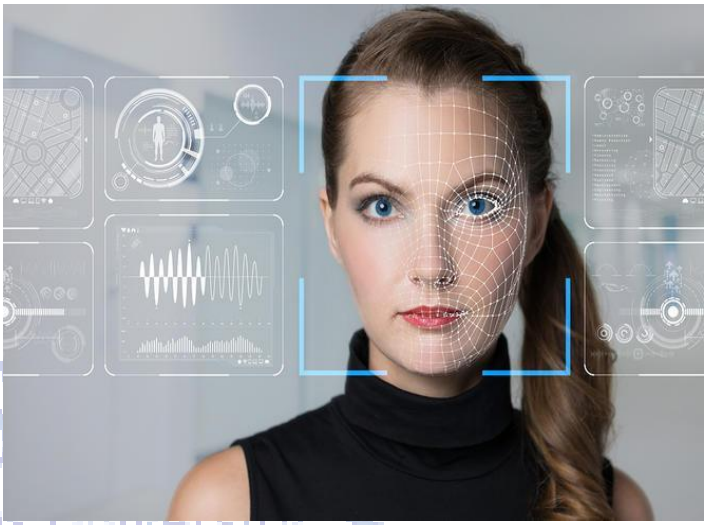
Although ITU is far older than the United Nations, it is fully integrated into the UN system. In 1947 it agreed to become a specialized agency of the UN. This means ITU acts independently but works closely with UN organs. For example, ITU reports to the Economic and Social Council (ECOSOC). This hierarchy of reporting paves a significant way for you, delegates to come up with solutions that need an active interaction with the UN's main bodies.

4. Introduction to the Agenda Item: Human Rights in the Age of Deepfakes and Synthetic Media

**What Are Deepfakes and Synthetic Media?**

Deepfakes are AI-generated synthetic media; audio, images or video produced by artificial intelligence that falsifies reality. For example, deepfakes can swap one

person's face for another in a video, or make someone appear to say or do something they never did. This technology emerged around 2017 and has immensely increased. Today, AI models can create realistic videos and even generate entirely new faces out of scratch. Such models are now easy to use and often very cheap, so now AI deepface use has increased dramatically.



**Concerns on Human Rights**

Impersonating someone or specific acts could cause global harm and can be a very significant malign in human rights. Therefore the United Nations with all its organs put work into combatting the deepfake technologies' use as a harmful tool. The internationally raised concerns pave the way for the efforts of enhancing this combat. Key concerns regarding the agenda are:

5. **Privacy Concerns:** Deepfakes often misuse a person's data without consent. Non- consensual sexual deepfakes are one upsettingly significant aspect. Such misuse violates rights to privacy and personal security and can be deeply traumatic for victims. Therefore, deepfakes can be used for identity theft or defamation of character in most cases.
6. **Informational Concerns:** Deepfakes are dangerous to the transmission of correct information because they cause fake news to be perceived as real, destroying people's faith in media and government officials. While disinformation should be combated, this should be done cautiously to prevent restricting free speech.

- **Minority Concerns:** Synthetic media often harms certain groups more than others, especially the disadvantaged ones. Most deepfake videos found online are sexual, and almost all of them target women. This means deepfakes are often used to harass women, especially public figures like celebrities. These fake videos are made without their permission and can lead to defamation of character.

7. Historical Background, Artificial Intelligence and Synthetic Media

Advances in machine learning, particularly deep neural networks, have made it possible to produce highly realistic synthetic images, videos, and sounds since

the 2010s. Since new generative models make it simple to create realistic multimedia content, the rapid development of AI has "escalated risks in the digital world to unprecedented levels." (ITU, 2023). The distinction between genuine and fake has become increasingly hazy, especially with regard to deepfakes, which are AI-generated media artifacts that effectively mimic a person's voice or likeness.

The technological origins of the phrase "deepfake" date back to 2014, when Ian Goodfellow introduced generative adversarial networks (GANs), a breakthrough that enabled AI to create increasingly realistic fake images (Westerlund, 2019). The term was first used in 2017 by a Reddit user who shared face-swapping films. These GAN-based generators served as the basis for contemporary synthetic media, along with associated autoencoder approaches. By the late 2010s, deepfake creation tools were readily available to non-experts because of the availability of massive datasets and powerful GPUs (Chesney & Citron, 2019).

Deepfakes' underlying technology development has happened gradually. Researchers created ever-more-advanced generative models following the 2014 GAN breakthrough. The StyleGAN family (2018–2020), for instance, is capable of creating artificial lifelike human faces (Westerlund, 2019). Neural generators for speech (e.g., WaveNet) and text (e.g., OpenAI's GPT series) developed simultaneously, allowing automated writing and realistic voice replication (Kietzmann et al., 2020). Open-source software and even smartphone apps made these deepfake technologies available to non-experts in the late 2010s and early 2020s (Schick & Witzleb, 2021). At the same time, research initiatives such as DARPA's Media Forensics, which was introduced in 2016, have been creating methods for identifying and evaluating media that has been altered by artificial intelligence (Chesney & Citron, 2019). Nevertheless, any improvement in generative quality makes detection harder.

**Societal Impact and Notable Incidents**

Deepfakes and synthetic media have extensive and complex societal repercussions that impact people, institutions, democratic processes, and public trust in general. The use of deepfake technology as a weapon to support gendered harassment and violence has been one of the most concerning

outcomes. About 96% of all deepfake movies on the internet were sexual, according to a 2019 study, and the vast majority of them targeted women without their knowledge (Schick & Witzleb, 2021). Non-consensual deepfake pornography victims may suffer from chronic psychological distress, damage to their reputations, and career difficulties. Deepfake content can have long-lasting effects on those who are impacted by its circulation due to its high shareability and difficulty in removal (Chesney & Citron, 2019).

By weakening trust in journalistic media and public discourse, the technology also poses a challenge to democratic institutions. Particularly during election seasons or violent situations, deepfakes can be used to mimic political figures, encourage violence, or create false occurrences. For example, deepfakes portraying candidates making controversial statements were shared online in the lead-up to elections in a number of nations, including the US and India, confusing voters (Paris & Donovan, 2019; Westerlund, 2019). The capacity to create convincing false news poses a threat to further destabilize political systems in democracies that are already characterized by a lack of trust in institutions (Kietzmann et al., 2020).

Deepfakes are dangerous for economic sectors in addition to politics. Deepfakes have been used to authorize fraudulent transactions and pose as executives in corporate settings. Cybercriminals deceived a UK-based energy company into sending €220,000 to a faux account in 2019 using AI-generated voice synthesis, one of the earliest recorded instances (Harwell, 2019). Because of the sophistication of these assaults, standard authentication techniques like speech recognition are no longer dependable, which increases the stakes for cybersecurity and corporate governance.

Furthermore, the usage of deepfakes in online fraud, disinformation, and social engineering is increasing. In order to deceive victims into thinking their loved ones are in danger, extortion schemes have employed AI-cloned voices of family members (Chesney & Citron, 2019). These psychological strategies take use of emotional susceptibility and show how deception produced by AI can function on both a mass and individual level. Deepfakes have been utilized to bring dead performers back to life in the media and entertainment sectors, sparking ethical

discussions about digital personhood, legacy, and consent (Kietzmann et al., 2020).

Lastly, it is impossible to ignore the psychological and epistemological effects of deepfakes. Citizens face a fundamental issue of trust in digital information in an era where reality itself can be artificially altered. In the end, this deterioration of "epistemic certainty"—the capacity to know what is true—may erode social engagement and democratic involvement by fostering political indifference, radicalization, or conspiracy theories (Schick & Witzleb, 2021; Paris & Donovan, 2019).

**Legal and Regulatory Developments**

These issues are now being addressed by governments and international organizations. Co-sponsored by 125 nations, Resolution A/78/L.49 on "safe, secure, and trustworthy AI" was adopted by the UN General Assembly in 2024 (United Nations, 2024). In the same direction, 193 states have approved UNESCO's 2021 Recommendation on the Ethics of Artificial Intelligence, which offers a worldwide framework for accountability and transparency in AI (UNESCO, 2021). To assist guarantee the authenticity of multimedia, standards groups like the ITU are actively debating technological standards like digital watermarking and content provenance systems (ITU, 2023).

The European Union has set the standard for regulation on a regional level. The world's first comprehensive AI law, the Artificial Intelligence Act, was finalized by the EU in 2023 and went into effect in August 2024 (European Parliament and Council, 2024). The Act places strict limits on "high-risk" applications and classifies AI systems according to danger. Importantly, it mandates that developers guarantee openness in AI operations and mark content produced by AI (European Parliament and Council, 2024). Fines for violations might reach 7% of worldwide sales. At the same time, online platforms are held responsible for damaging and unlawful content, including disinformation powered by artificial intelligence, under the EU's Digital Services Act, which goes into force in 2024.

Approaches have been scattered elsewhere. Congress in the United States has been cautious. Federal AI legislation is still pending, despite a 2019 addition to

the National Defense Authorization Act requiring a study of foreign deepfake risks (Chesney & Citron, 2019). A number of states in the United States have implemented specific legislation. For instance, Texas and California have prohibited some fraudulent deepfakes connected to elections, while Virginia, Georgia, and New York have prohibited non-consensual pornographic deepfakes (Schick & Witzleb, 2021). In order to forbid revenge-porn deepfakes and mandate that platforms reduce misinformation, the UK is revising its Online Safety Bill. In contrast, China's 2022 "Deep Synthesis" legislation mandate that agreement must be obtained before distributing certain deepfake content and that AI-generated media be properly labeled (Westerlund, 2019).

Industry organizations and IT corporations have also acted. TikTok revealed methods to identify and reveal AI-generated content in late 2023, while Meta (Facebook/Instagram) revealed watermarking and recognition capabilities for artificially created photos and videos in early 2024 (Kietzmann et al., 2020). To enable creators to add validated metadata to digital media, industry groups like the Coalition for Content Provenance and Authenticity (C2PA) are creating open standards. These steps are intended to provide consumers with a way to confirm whether an image or audio recording is authentic or artificially produced.

All things considered, the evolution of deepfakes exemplifies a traditional innovation cycle: quick technical advances are followed by a patchwork of societal and legal reactions. Every significant incident tends to draw attention from legislators and tech platforms, whether it's a multimillion-euro fraud case or a viral fake film during a geopolitical dispute. Although cooperative AI governance ideas are being discussed in international forums such as the ITU, OECD, and G7/G20, specific policies still differ by jurisdiction. Since deepfakes show how international norms and legislation must change in step with quickly expanding technology, they will probably continue to serve as a test case for AI governance.

8. Possible Solutions Regarding the Agenda

   Addressing the complex challenges posed by deepfakes and synthetic media requires a comprehensive, and layered approach that incorporates legal, technological, and educational strategies.

**Legal Regulations**: Governments, as the primary enforcers of legal frameworks, must introduce and uphold legislation that explicitly criminalizes the malicious use of deepfakes. This includes their use in identity theft, non-consensual pornography, defamation, and political manipulation. Laws should also ensure that victims have clear legal recourse and protection. Furthermore, cross-border cooperation is essential, as synthetic media can easily spread across jurisdictions, making international regulatory alignment a critical component of any legal solution.

**Technological Safeguarding**: Advancements in artificial intelligence should be matched by equal detection and authentication technologies. Investment in AI powered tools capable of identifying manipulated content through techniques such as anomaly detection, digital watermarking, and source verification is essential. Initiatives like the Content Authenticity Initiative (CAI) and the Coalition for Content Provenance and Authenticity (C2PA) aim to embed traceable metadata into digital files, helping verify their origin and integrity. Such tools not only assist in combating misinformation but also help build public trust in legitimate media.

**Public Awareness and Education**: As synthetic media becomes more advanced, educating the public is more important than ever. Media literacy programs should be integrated into school curricula, public campaigns, and online platforms to empower individuals with the critical thinking skills needed to detect and question potentially manipulated content. Awareness efforts must also address the ethical use of AI tools and encourage responsible digital behavior. When people understand the risks and learn how to verify content, they become the first line of defense against the spread of harmful synthetic media.

9. Major Parties Involved in the Issue

**a.Nation States**

**The United States of America**

Most artificial intelligence developers come from the United States (OpenAI and Meta). This made the USA the center of deepfake and synthetic media. Against this surging threat, some of the states in the USA have enacted legislation to regulate and curb this possible AI-threat. States such as Texas, Louisiana, Florida, South Dakota, New Mexico, Indiana, Washington, Tennessee, Oregon and Mississippi have criminalized deepfakes and any AI-generated images or videos that violate human rights.

**The People's Republic of China**

The PRC also contains a lot of tech giants such as Baidu, Alibaba, Tencent and ByteDance. They may not have become as strong as the USA yet but they have the largest database and one of the most developed IT infrastructure in the world. Also the support and funding of the government ensure the rapid development. But the regulations about AI and deepfakes are stricter in the country than the international usage. This brings us to the fact that Beijing has some strategies to conduct smear campaigns worldwide and influence the world.


**The Russian Federation**

The Russian Federation is not a world leader in AI like the USA or China. But they have been accused of intervening in the 2016 US elections and European politics. There are many state-sponsored trolls and bots that are being used for

controlling the public opinion. However they have prioritized the Military-AI usage.

**India**

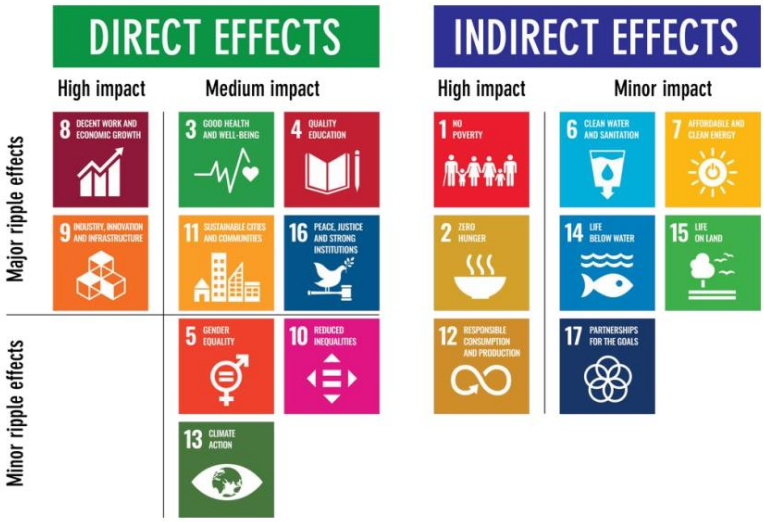
Like the People's Republic of China India has a vast population and as a result their database is also very large. Also there are human rights violations and usage of AI for manipulating the result of elections. But the government is trying to take legal precautions for that.

**b.International Organizations**



**United Nations Human Rights Council (UNHRC)**

UNHRC has been addressing and highlighting their concerns about this increase in deepfakes for years. UNHRC works to prevent deepfakes and misleading AI use that could lead to violations of people's right to privacy, harassment and slander, and violations of political rights.




**United Nations Educational, Scientific and Cultural Organization (UNESCO)**

UNESCO plays a crucial role for promoting the right and responsible usage of AI. They carry out projects such as guidance for global ethical framework and educating the public for the determination of deepfakes.

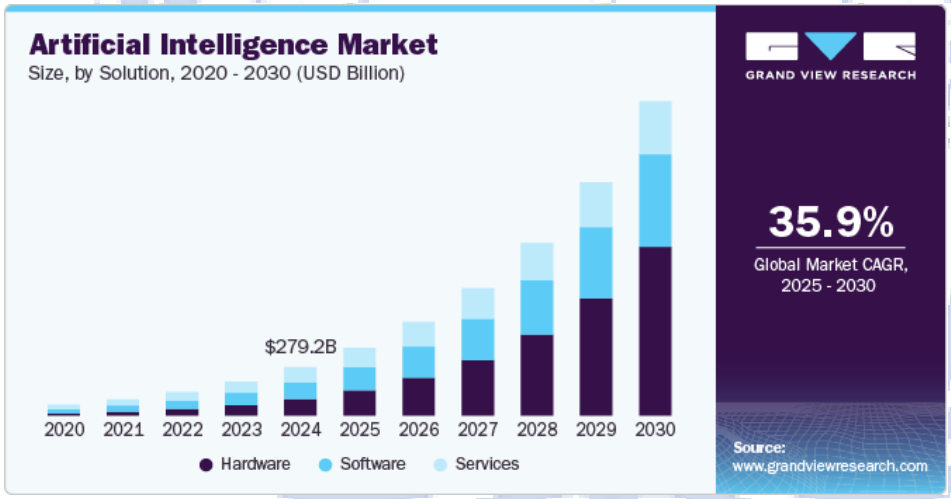
**INTERPOL and Europol**

They are enforcing the laws about deepfakes and trying to ensure human rights. In the Case Studies there is an example of an Europol operation which is Operation Cumberland. With that operation we can see that they take actions and the actions they take are influential.

**c.Technology Companies**

**OpenAI, DeepMind, Meta**

These are the forefront AI-tech companies which have programs that can generate realistic images, videos and texts. Although they may be used for educational purposes or creativity sometimes they cause more problems and conflict than they solve. As mentioned before they can lead to misinformation, non-consensual content, impersonation and public distrust. This even poses a greater threat because of the growth in the AI market.




**Social Media Platforms**

The distribution of deepfakes are as important as the generation of them. And these contents are usually released on platforms such as TikTok, Instagram, Facebook, Youtube or X. The decisive point here is their AI-detection tools and content moderation policies. Their regulations are different from each other.

10. Case Studies

a. **Political Manipulation**

**Deepfake video of Zelensky**


On March 16, 2022 an AI-generated video of Ukrainian President Volodymyr Zelensky was leaked. In this video the president was commanding his soldiers to surrender and lay down their arms. The purpose of the video was not only to make the soldiers surrender but dismantle the public trust in their president. This deepfake video has shown that it is possible to control the political views of people by distorting the truth and depicting them. But in reply to that Zelensky released a video in which he is saying "We are defending our land, our children, our families. So we don't plan to lay down any arms. Until our victory.". This reply proves that Zelensky had seen the threat and this video was not for amusement instead it was to manipulate and control the minds of people.This underlines the fact that artificial intelligence has the power to create conflicts and shape political views.

**The WIRED AI Elections Project**

The WIRED magazine has conducted a project named "The WIRED AI Elections Project" that evaluates the impact of AI on elections. They have detected 78 cases for AI usage. But when they analysed the content and intentions of these deepfakes they found that 39 of these uses are not to deceive the society. It reflects that AI may be used as a tool for campaigns and propagandas.

b. **Non-consensual Adult Content and Child Sex Abuse**

**Rana Ayyub**

In 2018, an Indian investigative journalist named Rana Ayyub has faced difficulties and human rights violations because of her opinions. After she condemned the Indian government and stood for the rights of an eight year old girl who was raped, she has experienced a online-hate campaign which involved the fabricated and AI-generated pornographic video of her. She was a victim of deepfake videos that were used for a smear campaign.

**Operation Cumberland**


In 2025, Europol has supported an operation which was related to the AI-generated child sexual abuse material (CSAM) distribution. This operation has led to the arrest of 25 suspects, the identification of 273 users worldwide, 173 seized electronic devices and 33 house searches. This operation was conducted in 19 countries and strengthened the opposition against CSAM and deepfake videos of children that were released by some criminal group members. And they earned money for fabricating videos that are violating human rights.

c. **Impact on business**

**CEO impersonation**

In 2019 a voice deepfake was used to scam the CEO of an unnamed UK-based firm. They received a call in which the caller used AI-voice technology to imitate the voice of the CEO in their parent firm. The scammer who was speaking like he was the CEO asked for $243,000. And the CEO in the UK-based firm has sent the money because they thought that the money was asked by their bosses.

**Explosion in Pentagon**


A deepfake image of an explosion at the Pentagon in 2023 caused a brief stock market decline after it was released. While this wasn't very harmful on its own, it did show how much trouble it could have caused if it had worked. A threat like this causes instabilities in the stock market.

11. Questions to be Answered

1-What legal frameworks can be used to implement the Connect 2030 Agenda goals?

2-What mechanisms can be developed to detect when deepfakes and synthetic media violate human rights?

3- How can international cooperation be strengthened in order to detect and prevent deepfake use and synthetic media?

4- In which ways public awareness can be raised in order to address the significance of combating deepfake and synthetic media?

5- Other than nation states, which members of the ITU could be held responsible regarding the agenda?

## 12. References


International Telecommunication Union. (n.d.). *About ITU*. Retrieved May 12, 2025, from https://www.itu.int/en/about/Pages/default.aspx

International Telecommunication Union. (n.d.). *History of ITU*. Retrieved May 12, 2025, from https://www.itu.int/en/about/Pages/history.aspx

International Telecommunication Union. (2023). *Measuring digital development: Facts and figures 2023*. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

International Telecommunication Union. (n.d.). *ITU sectors*. Retrieved May 12, 2025, from https://www.itu.int/en/ITU-R/Pages/default.aspx

https://www.itu.int/en/ITU-T/Pages/default.aspx

https://www.itu.int/en/ITU-D/Pages/default.aspx

United Nations. (n.d.). *Specialized agencies*. Retrieved May 12, 2025, from https://www.un.org/en/model-united-nations/specialized-agencies

ITU & UNESCO. (n.d.). *Broadband Commission for Sustainable Development*. Retrieved May 12, 2025, from https://www.broadbandcommission.org/

International Telecommunication Union. (n.d.). *Connect 2030 Agenda for global telecommunication/information and communication technology development*. Retrieved from https://www.itu.int/en/connect2030/Pages/default.aspx

International Telecommunication Union. (2023, October 16). *Deepfakes: Authenticity and transparency in the digital era*. ITU News. Retrieved from https://www.itu.int/en/ITU-T/AI/Pages/deepfake-authenticity.aspx

International Telecommunication Union. (2024, January 25). *ITU to launch multistakeholder focus group on AI watermarking and authenticity*. ITU News. Retrieved from https://www.itu.int/hub/2024/01/itu-focus-group-ai-watermarking-authenticity-deepfakes/

World Summit on the Information Society. (n.d.). *WSIS Process and Outcomes*. ITU. Retrieved May 12, 2025, from https://www.itu.int/net/wsis/

ITU. (2023). *ITU issues warning about rising threats from deepfakes and synthetic media*. International Telecommunication Union. https://www.itu.int

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11), 40–53. https://doi.org/10.22215/timreview/1282

Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs, 98*(1), 147–155. https://www.foreignaffairs.com/articles/2018-12-11/deepfakes-and-new-disinformation-war

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons, 63*(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11.006

Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence*. Data & Society Research Institute. https://datasociety.net

Schick, N., & Witzleb, N. (2021). Regulating deepfakes: Legal and ethical considerations. *Computer Law & Security Review, 41*, 105537. https://doi.org/10.1016/j.clsr.2021.105537

Harwell, D. (2019, March 7). A voice deepfake was used to scam a CEO out of $243,000. *The Washington Post*. https://www.washingtonpost.com