UNCSTD

[BACKGROUND GUIDE]

UN Comission On Science And Technology For Development

DPSIMUN ‘26

“Radical Resilienvce:Engineering Stability in an Age of Volatility”

Chairs

Arnav Pratap Maan,Hamida Abdul-Hamid

Committee]

UNCSTD

Contents

1.1 Welcome Message

Welcome delegates, to the UNCSTD at DPSIMUN 2026! Our main focus this year follows the conference theme “Radical Resilience: Engineering Stability in an Age of Volatility”. Essentially, our goal is to figure out how the global community can use technology to keep international systems stable when unexpected crises happen.

As representatives of your assigned nations, You'll be taking on some massive challenges—where emerging tech, global energy grids, cybersecurity, and economic growth all collide. We're looking for every delegation to bring sharp insights, jump into real debate, and build practical, forward-looking resolutions together.

1.2 Chair Messages

Arnav Pratap Maan CHAIR, UNCSTD

Hey everyone, welcome to UNCSTD (or you can just call it the CSTD) at DPSIMUN 2026! My name is Arnav Pratap Maan, and I am thrilled to serve as your Chair for this session, bringing my experience as a chair last year at the DPSIMUN 2025. Transitioning from being a delegate to chairing committees taught me that behind all the formal terminology and parliamentary procedure, the best MUN sessions come down to real engagement, strategic thinking and having some fun along the way.

As you prepare, keep in mind that quality will always beat quantity. You don't need to speak on every single motion to lead the room, as three well researched, policy heavy speeches addressing specific clauses will command far more respect rather than repeating the same points over and over again. I also encourage you to be a true bridge builder, because while it is easy to criticize another bloc's working paper, the strongest delegates are often the ones who can spot a conflict, find common ground, and dfart an actionable resolution that brings conflicting nations together. Finally, don't stress over the prep, take the time to understand your country's actual foreign policy, but never let inimidation hold you back, because every delegation has a voice in this room and committee is a lot more enjoyable when everyone is actively taking part in the debate.

Best Regards,
Arnav Pratap Maan

Hamida Abdul-Hamid CHAIR, UNCSTD

Hi everyone!
My name is Hamida and i'll be your chair for the CSTD committee at DPSIMUN 2026. As your chair for this years conference i bring experience as a seasoned MUN participant and a one time chair. I understand that it can be hard especially if you're a new delegate to understand how mun works, but as your co-chair i'm here to help everyone and give everyone equal opportunities. I encourage you all to do thorough research and have all the information and ammunition needed to make committee sessions fun and heated. I look forward to all the fun, debate and problem solving that is going to happen in this committee and i will do my part of making the committee fun for you all as well.

I want everyone to feel comfortable and feel free to reach out to me before the conference starts i will be available and willing to help.I look forward to meeting you all at the conference!

Best Wishes,
Hamida
Chair

1.3 Committee Overview

The United Nations Commission on Science and Technology for Development (UNCSTD) functions as a commission of the ECOSOC and serves as UN's main hub for science, technology and innovation (STI) for development. The CSTD offers member nations an organized platform to examine the swift advancements in technology and counsel the General Assembly on how to use innovation to further the 2030 Agenda for Sustainable Development.Designed to help member states navigate rapid technological transformation, the commission provides a structured intergovernmental forum to analyze emerging scientific trends, counsel the UN General Assembly and ECOSOC, and harness innovation to accelerate progress toward the 2030 Agenda for Sustainable Development. By bringing together policymakers, technical experts, and civil society, the CSTD translates complex technical developments into actionable international policy and governance standards.

Composed of 43 member states elected by ECOSOC for four-year terms, the CSTD serves as an inclusive intergovernmental platform that bridges technical expertise with high-level international policy. Supported substantively by the United Nations Conference on Trade and Development secretariat, the commission acts as the primary UN focal point for system-wide follow-up to the outcomes of the World Summit on the Information Society. In this capacity, the CSTD convenes delegates, civil society representatives, industry leaders, and academic panels between annual sessions to evaluate the societal impacts of frontier technologies, ranging from artificial intelligence and edge computing to digital connectivity and clean energy systems.

In alignment with our theme "Radical Resilience: Engineering Stability in an Age of Volatility", the UNCSTD discusses how structural differences in energy systems and internet access affect world stability. The commission works to create cooperative policy frameworks that safeguard susceptible infrastructure, deal with unequal acces to technology and set precise standards for emergency technology.Furthermore, the commission evaluates the geopolitical implications of energy decentralization, mitigates the dual-use risks of civilian platforms being repurposed for military operations, and creates mechanisms for rapid-response tech governance during catastrophic events. By democratizing access to critical computing power, satellite data, and hardware, the CSTD ensures that vulnerable states can independently build

Topic 1

Governance of Frontier Technologies for Crisis Response

Background Information

Creation of international rules governing frontier technologies such as artificial intelligence, automated drones and predictive analytics has generally lagged far behind the actual rate of technological development. Traditional non-proliferation arrangements, such as the Wassenaar Arrangement, had concentrated primarily on the regulation of physical hardware and weapons. With the growth of modern disaster relief and emergency logistics, however, increasingly dependent on private software and algorithms, the lack of standardized international rules became an issue that was easier to see than to overlook. The structural dependencies that developing countries have faced in accessing critical emergency tools are largely because of the concentration of advanced tech companies in developed nations. This lack of standardized global oversight exacerbates systemic vulnerabilities during catastrophic events. Because the research, infrastructure, and commercial control of advanced frontier technologies are heavily concentrated within private corporations in developed nations, developing countries face severe structural dependencies. During complex emergencies, low- and middle-income nations often find themselves reliant on external software providers, restricted by costly proprietary licenses, or subject to unilateral platform revocations. Furthermore, without clear international rules, humanitarian technologies deployed in crisis zones remain highly vulnerable to dual-use repurposing, state surveillance, and cyber exploitation, threatening both national sovereignty and civilian safety. Beyond data exploitation, dual-use technologies deployed under humanitarian pretexts risk being silently weaponized or integrated into military intelligence, surveillance, and target-acquisition systems. Without clear international rules, independent technical audits, and legally binding non-proliferation guardrails, the tools meant to deliver life-saving aid can inadvertently compromise national sovereignty and destabilize global security.

Historical Context

Historically, international regulatory frameworks governing frontier technologies such as artificial intelligence, automated drones, and predictive analytics have failed to match the rapid speed of technological innovation. Multilateral arrangements like the 1996 Wassenaar Arrangement were designed exclusively to monitor tangible physical assets, dual-use industrial machinery, and conventional weapons, leaving them ill-equipped to regulate intangible, cloud-hosted software and proprietary algorithms. As disaster relief, early-warning mapping, and emergency logistics migrated heavily to private digital systems over the past two decades, this governance void exposed severe structural inequalities. Because the research, computational power, and intellectual property driving these technologies remain concentrated within private corporations in developed nations, developing countries face deep structural dependencies. This leaves low- and middle-income states vulnerable to unilateral platform revocations, predatory licensing, unauthorized state surveillance, and the potential weaponization of dual-use humanitarian platforms during catastrophic events.

Current Situation

Today, the operational landscape of crisis response is defined by an accelerating race between private-sector technological innovation and fragmented global governance. Advanced predictive analytics, autonomous delivery drones, digital twin modeling, and cloud-hosted spatial mapping have become indispensable assets during complex emergencies. However, their deployment occurs almost entirely within an international regulatory vacuum. A primary driver of present-day instability is the extreme market concentration of foundational AI models, cloud compute, and low-Earth orbit satellite infrastructure within a small cohort of private multinational corporations headquartered in developed nations. When disasters strike, low- and middle-income countries routinely experience severe vulnerabilities, ranging from unauthorized demographic data harvesting and prohibitively expensive licensing fees to sudden, unilateral platform revocations during politically sensitive events. These dynamics demonstrate how technical dependencies actively undermine state sovereignty and national crisis readiness.

Concurrently, the operational boundary separating civilian humanitarian tools from state surveillance and military intelligence continues to dissolve. Dual-use software, algorithmic risk engines, and aerial mapping platforms deployed under the umbrella of disaster relief can easily be repurposed for target acquisition, civil monitoring, or offensive cyber operations. Without standardized technical audits, localized data encryption, or legally binding non-proliferation protocols, host nations face a stark dilemma: accept critical technological aid at the expense of national security, or reject advanced platforms and forfeit life-saving crisis capabilities. In response, multilateral bodies such as the UN Commission on Science and Technology for Development (CSTD) are attempting to formulate normative guardrails, establish emergency regulatory sandboxes, and build global compute-sharing banks. These initiatives aim to ensure that developing states can field frontier technologies during disasters safely, equitably, and without surrendering their data sovereignty.

Furthermore, these structural inequalities are exacerbated by algorithmic black-box opaque frameworks and the absence of standardized data sovereignty protocols. Emergency predictive models trained on biased datasets risk systematic misallocation of relief aid, routinely overlooking marginalized populations during critical post-disaster windows. Simultaneously, the rapid harvesting of biometric data, spatial mapping, and population telemetry by third-party vendor platforms leaves host states vulnerable to extraterritorial data exploitation. To mitigate these dual risks, international governance strategies are prioritizing zero-knowledge architecture, open-source algorithmic auditing, and hardware feature-locks to prevent civilian emergency tools from being converted into surveillance or tactical assets. By creating pooled UN compute banks, open technical repositories, and multilateral emergency transfer protocols, the CSTD seeks to dismantle monopoly bottlenecks, empowering developing nations to independently manage crisis response tech without remaining trapped in perpetual technological dependency.

Subtopics

Protection Against the Use of Dual-Use Tech

Legally designating emergency technologies like satellite broadband, AI mapping, and rescue drones as protected civilian assets guards them against military interference. Cryptographic locks, digital watermarking, and hardware air-gaps actively block these tools from integration into military targeting systems. Neutral verification bodies can then audit deployed humanitarian platforms in conflict zones to ensure they are not used for surveillance.

Establishing a Global Rapid Response Governance Council

A UN-aligned body provides an agile regulatory structure to manage the immediate deployment of advanced tech during catastrophic events. Activation relies on objective triggers, including UN Level 3 Humanitarian Emergencies and severe infrastructure failures. During active crises, the council issues time-bound legal indemnities, enabling humanitarian groups to field life-saving tools instantly without regulatory delays.

Mitigating Dual-Use Dilemmas

Standardized technical risk assessments evaluate emergency platforms prior to deployment to measure data sensitivity and security threats. Using zero-knowledge architecture and localized encryption ensures host nations maintain full ownership over sensitive demographic and spatial data. Role-based access controls and automated sunset clauses further protect systems by erasing operational data once the crisis ends.

The Global Tech-Divide in Crisis Response

Bridging global technology gaps requires an international resource bank that guarantees developing nations priority access to cloud infrastructure, satellite imagery, and processing power during disasters. Training local personnel to independently operate crisis systems builds long-term self-reliance. Additionally, international efforts must prioritize low-bandwidth, open-source infrastructure designed for resource-constrained environments.

Questions a Resolution Must Answer

1. Which specific UN body should oversee the international deployment of emergency technology during a crisis?

2. How can the international community verify that civilian humanitarian platforms are not being used for surveillance or military objectives?

3. What legal guardrails should be put in place to ensure host nations maintain data sovereignty when using foreign emergency software?

4. Under what specific conditions should emergency access or IP waivers apply to proprietary crisis technologies?

5. What objective criteria should define an official "crisis trigger" for rapid tech intervention?

6. How will technical training and hardware transfers be funded to help developing countries build their own crisis infrastructure?

Topic 2

Decentralised Power for A Volatile Future

Background Information

The transition toward decentralized power represents a critical shift from traditional, centralized power grids to distributed energy resources like rooftop solar, localized wind, battery storage, and smart microgrids. Centralized infrastructure is increasingly vulnerable to severe weather events, physical attacks, cyber threats, and global fuel price shocks. Decentralization mitigates these risks by allowing localized networks to island and operate independently during crises, ensuring continuous power for vital services. However, this transformation introduces complex governance challenges, including new supply chain dependencies on critical minerals, heightened cybersecurity vulnerabilities across millions of connected devices, and significant financial barriers for developing nations striving to modernize their energy infrastructure.

Historical Context

For most of the 20th century, modern power grids were developed around large, centralized power plants fueled by fossil fuels or large hydro projects. Rapid electrification was made possible by centralized grids, but this resulted in a system with single points of failure, leaving large regions vulnerable to major blackouts from severe weather or physical attacks. In the last two decades dramatic price reductions in solar, wind and battery storage have helped the growth of microgrids and localized power systems. However, the resources needed to move to decentralized grids have been unevenly distributed, leaving many developing economies still dependent on aging central infrastructure.

Current Situation

Extreme weather events, physical disruptions and sophisticated cyberattacks on critical infrastructure are raising the challenges for centralized energy grids. Localized microgrids are a type of decentralized system that increase energy reliability by enabling local power networks to run independently if the main grid fails. But the move to decentralized power shifts the landscape of global trade and the strategic dependencies that move away from oil and gas to critical minerals like lithium and cobalt. Additionally, connecting millions of Internet of Things (IoT) devices and smart meters to distributed networks significantly increases the overall cyber-attack surface.The global shift toward Decentralized Energy Systems (DES)including localized solar/wind microgrids, peer-to-peer (P2P) energy trading platforms, blockchain-secured smart grids, and localized battery energy storage systems (BESS)is no longer just a green transition strategy. It is now a critical national security and humanitarian survival imperative.

Subtopics

The Geopolitics of Energy Decentralisation

The shift toward critical minerals and smart-grid equipment reshapes global trade dynamics and introduces new supply chain vulnerabilities. Concentrated processing capacities and material shortages risk creating fresh geopolitical bottlenecks. Nations must diversify supply lines, establish strategic reserves, and formalize multilateral trade agreements to ensure stable access to essential components for localized energy infrastructure.

Bridging the Energy Digital Divide

Developing nations often lack the financial capital and technical infrastructure required to deploy localized smart grids. Targeted technology transfer and dedicated multilateral funding mechanisms are crucial for financing off-grid solar and microgrid projects. Prioritizing local workforce training ensures host communities can independently operate and maintain these decentralized systems long term.

The Security of Things: Managing the Vulnerable Edge

Distributed energy networks expand potential attack vectors by connecting thousands of edge IoT devices to central systems. Mandating baseline cybersecurity standards, zero-trust architectures, and automated firmware update protocols mitigates risks of grid disruption. Enforcing strict security protocols protects local energy management systems from unauthorized access, cyber espionage, and targeted sabotage.

Questions a Resolution Must Answer

1. What measures can UN member states take to build reliable, transparent supply chains for critical minerals needed in microgrid equipment?

2. What minimum cybersecurity requirements should be established for IoT devices operating within smart grids?

3. What financial frameworks can be used to support renewable microgrid projects in off-grid or rural areas?

4. How can the international community prevent market monopolies over smart-grid software?

5. How can technology transfers for clean energy software be managed while respecting intellectual property rights?

6. How can regional power networks safely integrate localized microgrids without risking overall system stability?

Glossary

Frontier Technologies: *Advanced, rapidly evolving technological tools—such as Artificial Intelligence (AI), autonomous robotics, and predictive analytics—that hold transformative potential across industries but often outpace existing legal and regulatory frameworks.*

Dual-Use Technology: *Hardware, software, or systems developed primarily for peaceful civilian or humanitarian purposes that can also be modified or repurposed for military, intelligence, or surveillance operations.*

Data Sovereignty: *The legal principle establishing that data collected within a nation's geographic boundaries is subject to the exclusive laws, governance, and judicial control of that specific host country.*

Compute Divide (AI Compute Gap): *The growing disparity between nations regarding access to high-performance computing hardware, massive data center infrastructure, specialized microprocessors, and processing power required to build and run advanced technological models.*

Decentralized Energy Infrastructure: *An energy generation and distribution network that produces electricity near the point of consumption using localized resources (such as solar or wind), operating either independently or in conjunction with a main grid.*

Microgrid: *A localized, self-contained energy grid that can operate connected to the traditional centralized power network or "island" itself to run independently during main grid failures or emergencies.*

Vulnerable Edge / Grid Edge: T*he perimeter of a decentralized digital network, encompassing connected Internet of Things (IoT) devices, smart meters, and localized sensors that interact directly with users or physical infrastructure, often presenting significant cybersecurity entry points due to minimal built-in security.*

Critical Information Infrastructure Protection (CIIP): *The strategic, technical, and regulatory policies designed to secure essential digital networks—such as power grids, telecommunications, and emergency software—from physical attack, failure, or cyber-threats.*

IP Waivers / Flexibility: *Temporary legal exemptions or modifications to Intellectual Property (IP) rights, patent laws, or commercial licensing terms during declared international emergencies, allowing developing or affected nations unhindered access to critical technologies or software.*

1.6 Refrences

United Nations Conference on Trade and Development (UNCTAD). (2023). Technology and Innovation Report: Highlighting Frontier Technologies and Sustainable Development. Geneva: UNCTAD.

United Nations Conference on Trade and Development (UNCTAD). (2025). Science, Technology and Innovation in the Age of AI (Issues Paper for the CSTD Inter-sessional Panel). Geneva: UNCTAD.

International Renewable Energy Agency (IRENA). (2024). Geopolitics of the Energy Transformation: Critical Minerals. Abu Dhabi: IRENA.

I**nternational Renewable Energy Agency (IRENA).** (2023). Low-Cost Renewable Power Generation and Microgrids for Remote Infrastructure. Abu Dhabi: IRENA.

International Telecommunication Union (ITU). (2024). Global Cybersecurity Index 2024: Strengthening National Cybersecurity Capabilities. Geneva: ITU.

International Telecommunication Union (ITU). (2022). Security Architecture for Internet of Things (IoT) Devices and Networks (Recommendation ITU-T Y.4806). Geneva: ITU.

UN Secretary-General. (2020). Roadmap for Digital Cooperation: Implementation of the Recommendations of the High-level Panel on Digital Cooperation. New York: United Nations.

United Nations General Assembly. (2024). Global Digital Compact (Annex to the Pact for the Future, A/RES/79/1). New York: United Nations.

Stockholm International Peace Research Institute (SIPRI). (2023). Dual-Use Export Controls and Emerging Technologies: Challenges for Multilateral Regimes. Stockholm: SIPRI.

Stockholm International Peace Research Institute (SIPRI). (2024). Protecting Critical Infrastructure Against Cyber Attacks: National and International Responses. Stockholm: SIPRI.

United Nations Office for Disaster Risk Reduction (UNDRR). (2023). Global Assessment Report on Disaster Risk Reduction: Resilience in an Age of Volatility. Geneva: UNDRR.

World Economic Forum (WEF). (2024). Harnessing Frontier Technologies for Disaster Risk Reduction and Humanitarian Action. Geneva: WEF.

World Economic Forum (WEF). (2023). Cybersecurity of Distributed Energy Resources: Protecting the Grid Edge. Geneva: WEF.