IMUN 2026 Research Report

General Assembly Issue #3: The question of strengthening cybersecurity in Less Economically Developed Countries.

Cybersecurity is "the collection of tools, policies [and safeguards] … that can be used to protect the cyber environment and organization and user's assets" (International Telecommunication Union). Less Economically Developed Countries (LEDCs) are "low-income countries confronting severe structural impediments to sustainable development" (United Nations Department of Economic and Social Affairs). As digital technologies are becoming increasingly entwined with economic growth and public services globally, LEDCs' limited infrastructure may increase their vulnerability to cyber threats.

There is a clear correlation between access to the internet and income: roughly ninety-three percent of people use the internet in More Economically Developed Countries (MEDCs), against only twenty-seven percent in LEDCs. Simultaneously, LEDCs are connecting faster than any other group, at roughly nine percent per year (International Telecommunication Union). On the other hand, LEDCs are ill-equipped for the quantity of users on online platforms, and lack the laws, technical agencies, and workforce required to ensure safety for all. Many LEDCs lack national Computer Security Incident Response Teams (CSIRTs), the primary measure to detect and respond to national cybersecurity incidents. As of 2024, only one third of countries in Africa had at least one operational CSIRT (World Bank Group). The International Criminal Police Organization (INTERPOL) found that cybercrime now makes up more than thirty percent of reported crime in parts of West and East Africa (INTERPOL). Because services like banking and government

operations rely increasingly on digital services, it is possible for a single breach to paralyze Member States.

The United Nations (UN) has built several frameworks to address this issue. The International Telecommunication Union (ITU) runs capacity-building programs and publishes the Global Cybersecurity Index, which ranks each country's development across several aspects of cybersecurity. In 2020, the General Assembly adopted resolution 75/240, creating an Open-Ended Working Group (OEWG) on ICT security. This initiative established voluntary norms and principles on cyber capacity-building and established a permanent UN Global Mechanism on ICT security (United Nations Office for Disarmament Affairs). The UN Convention against Cybercrime was adopted through resolution 79/243, and has over seventy signatory Member States, and is the first binding global cybercrime treaty (United Nations Office on Drugs and Crime).

MEDCs tend to favor voluntary norms backed by funding, training and technical assistance. LEDCs may push for stronger treaties, dedicated financing, and technology transfer. The Convention against Cybercrime remains controversial, as many Member States maintain that its broad surveillance powers invite abuse (Brown).

Delegates should focus on finding mechanisms that work to address the issue, rather than simply reaffirming LEDCs' vulnerability. Delegates should consider how to create and sustain national CSIRTs and cybercrime legislation in LEDCs, how to create predictable capacity-building, and how to share threat intelligence and electronic evidence across borders. Furthermore, debate may also be centered on inclusion of newly implemented conventions and ITU programs, and how to grow a cybersecurity workforce in regions facing severe skills shortages. Resolutions should be realistic for all Member States, respect

sovereignty and human rights, and should recognize that a breach in one weakly defended country has the potential to cascade across an interconnected region.

Works Cited

Brown, Deborah. "New UN Cybercrime Treaty Primed for Abuse." *Human Rights Watch*, 30 Dec. 2024, www.hrw.org/news/2024/12/30/new-un-cybercrime-treaty-primed-abuse.

International Telecommunication Union. "X.1205 : Overview of Cybersecurity." *Www.itu.int*, Apr. 2008, www.itu.int/rec/T-REC-X.1205-200804-I/en.

INTERPOL. *INTERPOL AFRICA CYBERTHREAT ASSESSMENT REPORT 2025 4 TH EDITION*. 2025, www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf.

United Nations Department of Economic and Social Affairs. "About the Least Developed Countries (LDC) Category | Economic Analysis and Policy Division." *Un.org*, policy.desa.un.org/least-developed-countries.

United Nations Office for Disarmament Affairs. "Open-Ended Working Group on Information and Communication Technologies (2021) | United Nations." *Meetings.unoda.org*, 2021, meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021.

United Nations Office on Drugs and Crime. "UN General Assembly Adopts Landmark Convention on Cybercrime." *United Nations : Office on Drugs and Crime*, 2021, www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html.

World Bank Group. "Enhancing Cyber Resilience in Developing Countries." *World Bank*, World Bank Group, 30 Jan. 2025, www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries.