Telecommunication
Development Bureau (BDT)

Ref.: BDT/DNS/CYB/DM/069

Geneva, 18 February 2025

- **ITU Member States of Africa region**
  Angola, Benin, Botswana, Burkina Faso, Burundi, Cabo Verde, Cameroon, Central African Republic, Chad, Congo, Congo (Dem. Rep), Côte d'Ivoire, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritius, Mozambique, Namibia, Niger, Nigeria, Rwanda, São Tomé and Príncipe, Senegal, Seychelles, Sierra Leone, South Africa, South Sudan, Tanzania, Togo, Uganda, Zambia, Zimbabwe
- **ITU Member States of Arab region:**
  Algeria, Comoros, Djibouti, Egypt, Libya, Mauritania, Morocco, Somalia, Sudan, Tunisia
- **ITU Member States of CIS region:**
  Armenia
- **ITU Member States of Europe region:**
  Albania, Bosnia Herzegovina, Georgia, Moldova, Montenegro, North Macedonia, Serbia, Ukraine
- **ITU Member States of Americas region:**
  Argentina, Brazil, Chile, Paraguay, Uruguay

Subject: **Invitation to participate in the 2025 cohort of *Her CyberTracks***

Dear Sir/Madam,

I am pleased to announce the third edition of the Her CyberTracks initiative, which will run from May to October 2025.

Her CyberTracks promotes the full, equal, and meaningful representation of women in cybersecurity by equipping women with the necessary skills and mindset to succeed in the field.

ITU-D and GIZ, in partnership with UNODC and EU CyberNet/LAC4, with the financial support of the Federal Foreign Office of Germany, will jointly undertake targeted cybersecurity capacity building activities for women by making available a six-month curriculum, giving participants access to trainings, networking opportunities and tailored mentorship with senior leaders in cybersecurity.

The program is poised to propel the next generation of women in cybersecurity into roles of leadership, ensuring that their voices and expertise shape the future of this critical field.

For this edition of Her CyberTracks, participation is open to women from a select number of countries in the Africa, Arab, CIS, Europe and Americas regions. A limited number of **fellowships** are available for each region to support participants in their travels. I take this occasion to invite our membership to disseminate the opportunity to potential participants that can benefit from this, as well as propose or nominate mentors and potential inspirational national speakers.

For further information and to register for the Her CyberTracks initiative 2025, please visit our website Her CyberTracks (itu.int).

If you have any queries concerning the programme, please write to: womenincyber@itu.int.

For more details on the initiative, registration, and eligibility criteria, please find the Terms of Reference along with the programme overview in the annex.

I look forward to the participation of the selected candidates and to a successful programme during the upcoming months.

Yours faithfully,

(Original signed)

Cosmas Luckyson Zavazava
Director

Annex 1: Terms of Reference

1. Introduction

Funded by the German Federal Foreign Office, the Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) and the International Telecommunication Union (ITU), in partnership with the United Nations Office on Drugs and Crime (UNODC) and the Latin America and Caribbean Cyber Competence Center (LAC4) have joined forces under the *Her CyberTracks* initiative to bridge the gender divide in cybersecurity.

2. Objectives

The objective of *Her CyberTracks* is to promote the equal, full, and meaningful representation of women in cybersecurity. To this end, the initiative equips women with the necessary skills and mindsets to succeed in cybersecurity through targeted cyber capacity building.

Her CyberTracks offers a one-stop curriculum based on three programme pillars:

- **TRAIN: Develop capacity to contribute to a secure and resilient cyberspace.** We provide expert training courses, delivered online and on-site, to equip women with the technical and soft skills needed to shape cybersecurity.
- **MENTOR: Promote awareness and knowledge sharing of best practices in cybersecurity career development**. We provide a platform for senior cyber professionals to mentor women at junior level and foster their professional and personal growth.
- **INSPIRE: Positive role models in cybersecurity inspire and empower further women to actively participate and lead in the field.** We organize inspirational keynote webinars, regional networking meetings and study visits to shift perceptions and (rightly) position women as valuable additions to the cybersecurity workforce.

3. Target audience & Foreseen Activities

The following three CyberTracks will be offered to the corresponding audiences:

CyberTracks	Target audience	Content and topics covered
Policy & Diplomacy CyberTrack	• Women in policy (cyber, ICT, peace & security) • Women in technical roles interested in policy/diplomacy.	• Concepts and processes of (inter-)national cybersecurity policy and diplomacy • Negotiation and public speaking • Cross-regional collaboration and information-sharing.
Incident Response CyberTrack	• Women working in IT wishing to enter cybersecurity. • Women at entry level in CERT/SOC teams.	• Cybersecurity concepts and basic incident management skills, including working with entry-level tools and techniques. • Communication and teamwork
Criminal Justice CyberTrack	• Women working in the criminal justice sector involved in or aiming to enter cybersecurity and countering cybercrime fields.	• Typologies and legal frameworks to understand and contribute to cybercrime cases investigations and prosecutions. • Communication and teamwork.

Through the MENTOR and INSPIRE pillars, all CyberTracks will cover professional development and networking.

All activities will be delivered between May and October 2025. GIZ and ITU jointly steer the global programme and implement the Policy & Diplomacy CyberTrack and Incident Response CyberTrack. UNODC implements the Criminal Justice CyberTrack, while LAC4 implements on-site activities for the Americas region.

4. Geographical coverage of eligible participants

Europe/CIS: Albania, Armenia, Bosnia and Herzegovina, Georgia, Moldova, Montenegro, North Macedonia, Serbia and Ukraine.

Africa: Angola, Benin, Botswana, Burkina Faso, Burundi, Cabo Verde, Cameroon, Central African Republic, Chad, Congo, Congo (Dem. Rep), Côte d'Ivoire, Equatorial Guinea, Eritrea, Ethiopia, Gambia, Ghana, Guinea-Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritius, Mozambique, Namibia, Niger, Nigeria, Rwanda, São Tomé and Príncipe, Senegal, Seychelles, Sierra Leone, South Africa, South Sudan, Tanzania, Togo, Uganda, Zambia and Zimbabwe.

Arab States: Algeria, Comoros, Djibouti, Egypt, Libya, Mauritania, Morocco, Somalia and Tunisia.

Americas: Argentina, Brazil, Chile, Paraguay and Uruguay (eligible for Incident Response CyberTrack only)

A limited number of **sponsorships** are available per region to support participants in their travels to on-site formats (e.g., face-to-face trainings and networking meetings) in their respective region.

5. Eligibility Criteria

To be eligible to participate in the *Her CyberTracks* initiative, interested women must have:

- For participants/"mentees":
    - **Policy & Diplomacy CyberTrack**: Minimum 2-3 years experience in the fields of policymaking/diplomacy, preferably in the fields of technology, cybersecurity and/or peace and security, or in technical cybersecurity fields
    - **Incident Response CyberTrack**: Minimum of 2-3 years experience in IT systems administration or < 1 year experience working in a public sector or (private) critical infrastructure sectors' computer emergency response team or security operations center. Participants should have basic system admin network skills and knowledge of Linux or Windows. For on-site training, participants should bring their own laptop.
    - **Criminal Justice CyberTrack**: Minimum 2-3 years experience in the criminal justice sector (e.g. prosecutors, law enforcement, lawyer, etc.)
- For mentors: Proven experience in the cybersecurity field, preferably senior and managerial positions in the public, private, justice, academic and civil society sectors.
- Participants must have a good working knowledge of English, as most courses will be held in English. Some parts of the Policy & Diplomacy Track curriculum will be available in French.
- Willingness and ability to allocate circa 10-15 hours per month for the duration of the programme.
- A computer and stable internet connection.
- There are no age restrictions.

Please note that participants from Argentina, Brazil, Chile, Paraguay, Uruguay can only apply to the Incident Response CyberTrack in 2025.

6. Additional Information:

- Programme seats are **limited and not guaranteed**.
- **Travel expenses are covered** for hands-on face-to-face trainings through a **limited number of sponsorships** for participants from the target countries.
- The programme will be delivered through ITU Academy and on-site.
- Selected applicants will be contacted by email starting end of April 2025.
- Upon completion of the programme, participants will receive a certificate.

7. Application form & registration

Applications for participation in the *Her CyberTracks* initiative 2025 will be accepted until 31 March 2023. **Please apply for the programme via the following links:**

Policy & Diplomacy CyberTrack: apply here

Incident Response CyberTrack: apply here

Criminal Justice CyberTrack: apply here

For mentors, application is done via the following link.

Information about registration and logistics concerning the programme offers and timeline will be posted on the *Her CyberTracks* programme webpage.

8. Contact details

If you have any questions, please feel free to contact: womenincyber@itu.int

Or our ITU regional representatives:

Regional Office for Europe, Mr. Jaroslaw Ponder: Jaroslaw.ponder@itu.int
Regional Office for the Africa region, Mr. Serge Valery Zongo: Serge.zongo@itu.int
Regional Office for the Arab region, Mr. Adel Darwish: adel.darwish@itu.int
Regional Office for the Americas, Mr. Pablo Palacios: pablo.palacios@itu.int

9. About our partners

GIZ (www.giz.de/en)

As a service provider in the field of international cooperation for sustainable development and international education work, the Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) is dedicated to shaping a future worth living around the world. GIZ has over 50 years of experience in a wide variety of areas, including economic development and employment promotion, energy and the environment, and peace and security. GIZ is present in 120 countries. Since 2023, GIZ implements the Partnership for Strengthening Cybersecurity project on behalf of the German Federal Foreign Office and with support of the European Commission. The project aims to reinforce selected bilateral and regional partners' capabilities to prevent, mitigate and respond to cybersecurity threats, and to improve collaboration of strategic partners with Germany to protect the global cyberspace.

UNODC (https://www.unodc.org)

The mission of the United Nations Office on Drugs and Crime (UNODC) is to contribute to global peace and security, human rights and development by making the world safer from drugs, crime, corruption, and terrorism, UNODC works for and with Member States to promote justice and the rule of law. The important

and complementary mandates of UNODC distinguish the Office from others in the same field: serving as the guardian of international conventions and the secretariat to global policy bodies; providing strong research and policy analysis; and combining global expertise and a wide field presence to provide specialized assistance to Member States. Since 2013, the UNODC Global Programme on Cybercrime is supporting Member States in strengthening their response against cybercrime by providing policy analysis, capacity building for the criminal justice sector, prevention expertise and by facilitating international cooperation in countering cybercrime.

LAC4 (https://www.lac4.eu)

The Latin American and Caribbean Cyber Competence Center (LAC4) is a collaborative platform dedicated to enhancing cybersecurity resilience and capacity in the Latin American and Caribbean (LAC) regions. It serves as a hub for fostering partnerships between governments, private sectors, academia, and civil society to address shared cybersecurity challenges. By promoting initiatives like workforce development, secure connectivity, and multistakeholder collaboration, LAC4 aims to strengthen critical infrastructure and develop regional expertise in cybersecurity. It also plays a key role in bridging efforts between the LAC region and the European Union for global cybersecurity resilience. LAC4 is implemented by EU CyberNet and funded by the European Union.