Principal Cyber Diplomacy Officer – GIZ African Union Partnership for Strengthening Cybersecurity II to be seconded to the AUC Defense and Security Governance Division, Political Affairs, Peace and Security Department

Position:	Principal Cyber Diplomacy Officer
Place of Assignment:	Addis Ababa, Ethiopia
Initial Contract Period:	01.10.2024 – 31.12.2025 (with a possibility of extension)
Application Deadline:	21 July 2024

About GIZ

The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH is a global service provider in the field of international cooperation for sustainable development dedicated to shaping a future worth living around the world. As a public-benefit federal enterprise, GIZ supports the German Government – in particular the Federal Ministry for Economic Cooperation and Development (BMZ) – and many public and private sector clients in achieving their objectives in international cooperation in around 120 countries.

Since 2004, GIZ has been a reliable and trusted partner of the African Union (AU) to enhance inclusive growth and sustainable development on the African continent in line with the AU's Agenda 2063: The Africa We Want. With more than 200 staff, GIZ African Union cooperates with the AU Commission, as well as the AU's specialised institutions and agencies, such as the Development Agency AUDA-NEPAD, at continental, regional and national level in more than 35 member states. Key areas of engagement include Peacebuilding and Conflict Prevention, Governance and Migration, Sustainable Economic Growth and Employment, as well as Health and Social Development.

The African Union Commission (AUC) and the German Federal Foreign Office have expressed the willingness and interest to strategically cooperate in the field of cyber diplomacy and strengthen African capacities and resilience in cybersecurity.

The Global Project "Partnership for Strengthening Cybersecurity" has been commissioned by the German Federal Foreign Office in 2023. Its main goal is the reinforcement of selected bilateral and regional partners' capabilities to prevent, mitigate and respond to cyber security threats. Its regional components focus on the African Union (AU), the Economic Community of West African States (ECOWAS), as well as the Western Balkan and Eastern European countries. The project is implemented GIZ in close cooperation with regional political partners, and co-funded by the European Commission since 2024.

With the AU Commission, the project aims to contribute to a) developing cyber diplomacy mechanisms and skills, as well as operationalising cybersecurity norms and policy frameworks at AU and member state level; and b) enhancing the AUC's strategic and operational cybersecurity capacity.

Core Tasks

The GIZ project “Partnership for Strengthening Cybersecurity” is seeking a highly qualified **Principal Cyber Diplomacy Officer** to be seconded to the AUC’s Political Affairs, Peace and Security Department. The Officer will provide the strategic and operational expertise for the implementation of tasks and activities related to advancing the AU’s cyber diplomacy profile both through AU bodies and with member states.

Where appropriate and reasonable, you perform further tasks assigned to you by your line manager outside the scope of the job description.

Main Activities

Responsibilities and Duties

- Under the direct supervision of Head of Defense and Security Governance, the Principal Cyber Diplomacy Officer will be responsible for the direction, planning and management of all activities related to the engagement of African Union in the arena of cyber diplomacy.
- Concrete responsibilities include understanding and mapping multilateral processes that shape the global cybersecurity agenda, building alliances and collective response to cyber threats through diplomatic means, negotiating cooperative frameworks, fostering capacity building, and promoting the application of human rights and international law in the cyber space.
- The officer further needs to facilitate and ensure coordination with other AU actors involved in cybersecurity, particularly the AU Cybersecurity Expert Group, the AU Commission on International Law, and further related AUC departments.

Functions

- Coordinate, support and oversee the implementation of activities to advance the cyber diplomacy profile of the AUC, continental awareness of cybersecurity as a (foreign) policy field, as well as member state capacities in cyber diplomacy, e.g. regarding the development and implementation of cybersecurity norms and frameworks.
- Prepare policy documents, strategic guidelines and operational work plans for the division’s work on cyber diplomacy and follow-up on their implementation.
- Prepare cyber diplomacy reports and support documentation for the Peace and Security Council.
- Stimulate and coordinate exchange with member state cyber diplomacy focal points in both capitals and relevant delegations.
- Coordinate with cybersecurity structures and relevant political actors on potential diplomatic tools or responses to cyber incidents at AU or member state level.
- Team up with other AUC departments to develop and promote a joint understanding of AU priorities and actions on cybersecurity.
- Identify and coordinate international partners which (may) collaborate with AU in the area of cyber security, such as international organizations, NGO, governments or private sector.

Qualifications

Qualifications

- Master’s degree or an advanced university degree in the field of political science or business economics, international relations, IT security or computer science or a comparable field relevant to the position and subject area. A first university degree in combination with strong qualifying experience may be accepted in lieu of Master’s degree or the advanced university degree.
- Strong understanding of cyber conflict, international cyber policies and norms, including legal and ethical factors, and actors and motivations involved in cyber incidents.
- Professional proficiency in English (orally and written) is required, knowledge of French and other languages of the African Union are an asset.

Experience

- A minimum of eight years progressive professional experience in the field of cyber diplomacy, international relations, cybersecurity policy or a related field is required, including at least five years of international experience, in either public or private sector.
- A minimum of three years in a senior or management position in a related area.
- Experience in diplomatic practice is a strong advantage.
- Previous experience in effectively coordinating complex inter-departmental/inter-institutional change processes with the necessary skills in facilitation and leadership of non-hierarchical teams.
- Excellent knowledge of the workings of international organizations.

Skills

- Ability to develop and delegate clear programme goals, plans and actions, including budgets, that are consistent with agreed strategies and focus on sustainable implementation.
- Excellent analytical, drafting and report writing skills, as well as planning and organizational skills, combined with the ability to work independently and self-reliantly.
- Strong interpersonal, problem-solving and communication skills, both written and verbal, and a cooperative and supportive team spirit.
- Capacity to work under pressure in a multicultural environment, and a demonstrated ability to initiate and promote collaborative approaches between geographically and culturally disparate partners.
- Ability to establish and maintain effective partnerships and working relations both internally and externally.
- Strong sense of credibility, impartiality, and unconditional discretion with an interest to having a commitment to life-long learning and staying up to date with cybersecurity and threat-related trends.

HOW TO APPLY

The application should include

- a motivational letter / letter of application,
- a recent CV, including at least three referee contacts.

Applications should be submitted via email to **hr_au@giz.de** with the subject line **“Principal Cyber Diplomacy Officer – AUC PAPS– Your Name”**.

Closing date for applications: **21 July 2024, midnight EAT.** Only Shortlisted Candidates will be contacted.

GIZ is an equal opportunity employer and welcome applications from individuals regardless of gender, disability, race, ethnicity, religion, age, or any other protected characteristic. We embrace diversity and believe that inclusivity in the workplace is essential to our success and we are committed to creating a work environment where all employees are valued and respected.