Senior Cybersecurity Officer to be Seconded to the African Union Commission (AUC) Political Affairs, Peace and Security Department – GIZ African Union Partnership for Strengthening Cybersecurity Program

Position:	Senior Cybersecurity Officer
Place of Assignment:	Addis Ababa, Ethiopia
Initial Contract Period:	01 June 2025 – 31 December 2026
Salary Band	The position is assigned to GIZ Salary Band 4 which is equivalent to AU P3
Application Deadline:	30 March 2025

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 around 250 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 40 member states. Key areas of engagement include Peacebuilding and Conflict Prevention, Governance, Sustainable Economic Growth, Health and Social Development, as well as Just Transition.

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 by GIZ in close cooperation with regional political partners, and co-funded by the European Commission since 2024.
Based on a joint partnership between the AU Commission and the German Federal Foreign Office, the project aims to contribute to the AUC's strategic and operational cybersecurity capacity and to developing and operationalising cybersecurity norms and policy frameworks at continental and member state level.

Core Tasks

As part of the joint partnership, GIZ is seeking a highly qualified **Senior Cybersecurity Officer** to be seconded to the AUC's Defense and Security Governance Division (DSG), within the Political Affairs, Peace and Security Department.

At various occasions over the past years, the AU Peace and Security Council (PSC) expressed concern over the growing threat to peace, security, and stability on the Continent due to increasing cyber threats and reiterated the importance of cyber security in security governance. It requested the AU Commission to establish a Unit within the Political Affairs Peace and Security (PAPS) Department, which will work together with all other stakeholders in monitoring and reporting on cyber-security issues within the Continent.

In line with AU core values and as part of the Defense and Security Governance Division, the Senior Officer will provide technical support in the development of AU cybersecurity programmes in the area of political affairs, peace and security, to operationalize relevant cybersecurity and Artificial Intelligence (AI) norms and policy frameworks at AU and Member States level, in line with PSC decisions and the implementation of the AU Convention on Cyber Security and Personal data protection.

The Senior Officer will provide the strategic and operational expertise for the implementation of tasks and activities related to advancing the AU's cybersecurity and Artificial Intelligence (AI) profile in the area of political affairs, peace and security, in close collaboration with other relevant AUC units, both through AU bodies and with member states.

Main Activities

Main Functions and Responsibilities

- Provide technical and strategic support to the Governance and Conflict Prevention Directorate at the AU Commission, through the DSG Division, in planning and management of all activities related to the engagement of the AU in the area of cybersecurity and AI from a political affairs, peace and security perspective
- Support AU Member States, Regional Economic Communities (RECs), and Regional Mechanisms (RMs) per their requests in strategic policy, legal and regulatory issues related to cyber and AI from a political affairs, peace and security perspective.
- Provide technical support to improve continental cyber diplomacy awareness, mechanisms and skills, including raising awareness on main cyber developments and ongoing cyber and AI negotiations at global level, and trainings to increase cyber diplomacy knowledge and skills for ministerial and diplomatic staff in member states and relevant missions.
- Understanding and mapping multilateral processes that shape the global cybersecurity and AI agenda, building alliances and collective responses to cyber threats, negotiating cooperative frameworks, fostering capacity building, and promoting the application of human rights and international law in cyberspace.
- Provide technical support to PAPS Department to ensure coordination with other AU actors involved in cybersecurity, particularly the AU Cybersecurity Expert Group, the AU Commission

on International Law, AFRIPOL, AU Center on Counterterrorism, as well as relevant AUC departments, AU specialized institutions and organs.

Specific responsibilities include the following:

- Coordinate and support the implementation of activities to advance the cybersecurity profile of the AUC from a political affairs, peace and security perspective, as well as Member State capacities in the development and implementation of cybersecurity norms and frameworks, in close collaboration with RECs/RMs.
- Provide general advice and guidance on strategic aspects of other portfolios linked to cybersecurity including Artificial Intelligence
- Prepare policy documents, strategic guidelines and operational work plans for the division's work on cybersecurity and diplomacy and follow up on their implementation.
- Prepare cybersecurity reports and support documentation for the Peace and Security Council and other relevant AU Policy Organs.
- Stimulate and coordinate exchange with Member States cybersecurity focal points and agencies in both capitals and relevant delegations, particularly those with a peace, security and diplomacy perspective.
- Coordinate with other cyber structures and relevant political actors on potential diplomatic tools or responses to cyber incidents at the AU or Member states level.
- Team up with other AUC departments to develop and promote a joint understanding of AU priorities and actions on cybersecurity and diplomacy.
- Identify and coordinate international partners which (may) collaborate with AU in the area of cybersecurity, such as international organizations, NGO, governments or the private sector.
- Undertake other peace and security-related duties as assigned by the Head, DSG Division, Director, Governance and Conflict Prevention or Commissioner for Political Affairs Peace and Security (PAPS).

Qualifications

Qualifications

- Master's degree or an advanced university degree in the field of political science or business economics, international relations, 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, fluency in another AU language (Arabic, French, Portuguese) is an added advantage.

Experience

- Demonstrated experience of at least five (5) years in the development and implementation of strategic policies and programmes related to cybersecurity in Africa, within international or regional organizations, with active engagement of governmental decision-makers, is required.

- Additional experience in the area of Artificial Intelligence would be a valuable assetprocesses with the necessary skills in facilitation and leadership of non-hierarchical teams.
- Additional experience as an IT Officer would be a valuable asset.
- A minimum of three years in a senior or management position in a related area.
- Experience in international relations or diplomatic contexts is a strong advantage.
- Experience in effectively cooperating in complex cross-cutting settings with the necessary skills in facilitation 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, while being conscientious in observing deadlines and achieving results.
- 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, in a culturally sensitive environment.
- 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 **“Senior Cybersecurity Officer – Your Name”**.

Closing date for applications: **30 March 2025, 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.