Concept Note

Advancing Cybersecurity and Cyber Diplomacy in Africa

1. Introduction

The United Nations Economic Commission for Africa (ECA), in partnership with the Global Network for Cybersolution (GNC), will organize a comprehensive Two-Day High-Level Webinar entitled "Advancing Cybersecurity and Cyber Diplomacy in Africa". This high-level webinar program is strategically designed to translate global digital policy into actionable, harmonised strategies across the African region.

2. Background

On 5 July 2012, the UN Human Rights Council (HRC) adopted by consensus a key resolution on promotion, protection and enjoyment of human rights on the Internet (UN Doc. A/HRC/20/L.13).The protection of citizens' right is a security concern affirmed by the Universal Declaration of Human Rights, adopted by the United Nations in 1948. Therefore, the need to assure online security (a.k.a. Cybersecurity) of citizens cannot be over-emphasized.

Currently, over 5.35 billion people worldwide use the internet, representing approximately 66% of the global population as of early 2024. Billions of devices—including systems, sensors, and actuators—operate autonomously within the context of the Fourth Industrial Revolution (4IR). According to recent reports from Statista and the World Economic Forum (WEF), there are now over 30 billion devices connected globally. As connectivity continues to expand, the prevalence of online risks is expected to increase, underscoring the urgent need for robust security measures to maintain trust and confidence. These efforts are essential to support ongoing initiatives related to the Sustainable Development Goals (SDGs) 2030 and the African Union (AU) Agenda 2063: The Africa We Want.

Hence, Cybersecurity is a concern for all stakeholders: government, the private sector, civil society, the technical and academic communities, and young people within the multi-stakeholder Internet ecosystem. For a region such as Africa which remains the least digitalised globally—the core of the challenge revolves around two closely linked issues: trust and security. According to Interpol's African Cyberthreat Assessment Report 2024, cybercrime is responsible for an estimated annual loss of over $4 billion across the

continent, continuing to negatively impact GDP and per capita income. Recent estimates indicate that more than 90% of African businesses still lack adequate cybersecurity protocols. In Nigeria, cybercrime remains a significant issue, with the Economic and Financial Crimes Commission (EFCC) reporting that in 2023, over 70% of its convictions were related to cybercrime. The country faces more than 70,000 cyberattacks daily, with annual financial losses now exceeding $500 million. Similarly, annual losses attributed to cybercrime in South Africa are estimated at approximately $600 million, while Kenya reports losses in the region of $50 million per year. In summary, the principal challenge for cybersecurity in Africa remains the lack of comprehensive, professional assessment of vulnerabilities at both top-down and bottom-up levels, alongside the need for stronger political will and determination across all sectors to address these weaknesses.

Additionally, African nations continue to encounter considerable obstacles in the sphere of cyber diplomacy and struggle to participate effectively in international cyber governance initiatives aimed at ICT security. The continent remains notably underrepresented in these diplomatic forums, including the United Nations' ongoing efforts to establish cyber norms. Although the UN Group of Governmental Experts (GGE) claims to select members based on fair geographic representation, African involvement has historically lagged behind that of other regions; since 2004, only eight African countries have been included in the GGE's membership. Despite meaningful progress made by both the GGE and the Open-Ended Working Group (OEWG) on cyber governance discussions, the specific conflict and security challenges facing various African areas have not been adequately addressed. Moreover, the limited number of skilled cyber diplomats in African countries continues to restrict the continent's capacity to advocate for its interests in cyber diplomatic negotiations[1].

3. Objectives

The webinar is designed to address the unique challenges facing African nations in the digital sphere, including the increasing prevalence of cyber threats, the urgent need for robust security protocols, and the importance of effective participation in global cyber governance.

The programme will:

- Provide information about current cyber threats and major cybersecurity priorities and facilitate discussions among various communities regarding the nature and scope of these threats.
- Facilitate the exchange of knowledge, best practices and successful operations conducted within the African continent.
- Review recent developments and current issues in cyber diplomacy, highlighting efforts to increase African involvement in global cyber governance and policymaking.

[1] African Union (2018) Cyber Security and Cybercrime Policies for African Diplomats Cyber Security and Cybercrime Policies for African Diplomats | African Union (au.int)

- Build capacity among African diplomats to engage in cyber diplomacy and navigate the complexities of cybersecurity
- Include a panel discussion featuring cybersecurity specialists who will highlight opportunities and respond to participant inquiries.

4. Target Audience

This collaborative initiative aims to bring together policymakers, cybersecurity professionals, diplomats, civil society representatives, and members of the technical and academic communities from across Africa and beyond. Participants will benefit from a series of expert-led discussions, case studies of successful operations within Africa, and interactive sessions aimed at building the skills and networks needed to safeguard the continent's digital future.

5. Expected Outcomes

The webinar will produce a shared, forward-looking agenda to guide Africa's cybersecurity and digital diplomacy efforts. It aims to:

- Foster regional cooperation and policy coherence in cybersecurity governance
- Strengthen institutional and diplomatic capacity for cyber engagement
- Support capacity-building and knowledge exchange on digital trust, AI, and emerging tech
- Lay the groundwork for regional agreements and frameworks promoting a secure, inclusive, and trustworthy digital future.