UNODA ICT Mapping Exercise: Cyber Capacity Building

Mapping Germany's approach to CCB and its existing initiatives in cyber space

Digital transformation introduces both new opportunities as well as risks and vulnerabilities that need to be considered and addressed by states, organizations as well as citizens. Digital technologies are used to attack critical infrastructure, interrupt digital services, commit cybercrime, increase surveillance, commit human rights abuses, and spread disinformation. This, in turn, has severe negative impacts for individuals, economy, society and public institutions as well as overall stability in global cyberspace.

Bearing this development in mind, **Germany** through the **German Federal Foreign Office** actively promotes international cybersecurity policies for a global, open, free, inclusive, stable, and secure cyberspace. It is committed to work closely with relevant organizations, partners and stakeholders to increase cyber resilience, strengthen cybersecurity capacities and the international cybersecurity architecture.

Moreover, all our cyber capacity building (CCB) work is following a partnership-based approach and seeks to enhance regional cooperation, which we deem a key requirement for states to effectively detect, defend against or respond to malicious ICT activities. Germany further places a strong emphasis on implementing its CCB activities based on the agreed UN Framework including the principles for cybersecurity capacity building and implementing the norms of responsible state behavior in cyberspace.

Germany's guiding principles in CCB

To illustrate how this can look in practice, Germany advocates that the International Community should work together by promoting regular collaboration and information sharing to avoid gaps and asymmetries in cyber capacity building, which includes sharing best practices, identifying and addressing vulnerabilities as well as identifying and adopting common frameworks and standards.

Further, Germany is convinced that sharing the same objectives is key for effective coordination of capacity building initiatives and to avoid duplication of efforts, while a demand-driven approach with local ownership is vital to make capacity building engagement the two-way street it is essentially supposed to be.

Moreover, capacity building should never lose sight of the technical foundations, while at the same timing advancing in an action- and practitioner oriented manner. Finally, it is essential to get all stakeholders from different sectors and fields into the same room if we want to take on a comprehensive and holistic approach to cyber capacity building**.**

Existing Initiatives under the umbrella of Germany's CCB strategy and priorities

To support this endeavour, the **Partnership for Strengthening Cybersecurity** has been created in 2023 as one of the German instruments to provide technical capacity, foster partnerships and increase public awareness. Its aim is to effectively contribute to the global network of likeminded cooperation partners and to advance cyber capacity building. The programme is being implemented by Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) on behalf of the German Federal Foreign Office.

The rationale of the programme is to contribute to capacities of partner countries to assume increased responsibility for their cybersecurity. Its main goal is the reinforcement of selected bilateral and regional partners' capabilities to prevent, mitigate and respond to cyber security

threats and the further development of Germany's cooperation with strategic partners in this area. The regional components of the scalable global project approach initially focus on the Economic Community of West African States (ECOWAS), the Western Balkan and Eastern Europe. The focus of each component is as follows:

- **ECOWAS:**

Under Germany's G7 Presidency, the Joint Platform for Advancing Cyber Security was launched by the ECOWAS Commission to strengthen the cyber resilience of the region. The corresponding Action Plan (2022 – 2025) of the Joint Platform provides concrete priority areas that allow the ECOWAS Commission to structure its cooperation with global, regional, and national partners to carry out capacity building and regional coordination initiatives in the area of cybersecurity. These include strengthening cyber diplomacy mechanisms and skills; protection of critical infrastructures; protection of vulnerable groups against cybersecurity threats; and data sovereignty.

- **Western Balkans:**

Under the umbrella of the Berlin Process, all dedicated partner countries decided to establish a partnership with the Western Balkan countries to strengthen cybersecurity in the region via enhanced regional cooperation and support these countries on their road to EU membership. The cooperation shall respond to the regional needs and foster regional exchange and mutual learning on the subject.

- **Ukraine:**

In Ukraine, together with Ukrainian public authorities, Germany is developing a National Training Program of Cybersecurity for professionals working in the public sector. The objective of the programme is to support Ukraine in aligning with European Union cybersecurity standards and requirements, thereby increasing the cybersecurity of the European neighborhood and, ultimately, cybersecurity throughout democratic societies in the whole of Europe.

- **Her CyberTracks**

Throughout all regions, Germany is also committed to promoting a feminist foreign policy. This includes investing resources into promoting the equal, full, and meaningful representation of women in the field of cybersecurity. The Partnership for Strengthening Cybersecurity contributes to that aim through a dedicated project 'Her CyberTracks', which is implemented jointly with ITU on a global scale, with a particular focus of activities in the selected regions.

Her CyberTracks aims to promote the representation and participation of women seeking to enter and/or advance in international cybersecurity policy processes and diplomacy. To that end, the initiative makes available a complementary and one-stop holistic curriculum. Women will be enabled through capacity development, inspired through role models and networking, and empowered through tailored mentorship with senior women leaders in cybersecurity. Her CyberTracks leverages existing offerings for cyber capacity building from the partner network, capitalizes on complementary strengths, and avoids duplication.

Other projects as part of Germany's international CCB initiatives include the following:

- **Strengthening Cybersecurity Capacities in Bosnia and Herzegovina (with UNDP):**

This project aims to strengthen cybersecurity capacities in Bosnia and Herzegovina by identifying and assessing domestic resources and establishing coordination mechanisms. Through this project, UNDP and regional actors create a cybersecurity agenda and develop a regulatory and institutional framework to strengthen IT-infrastructure against cyber-attacks.

- **World Bank Digital Development Partnership**

Germany has been a key contributor in the established Cyber Security Multi-Donor Trust Fund of the World Bank strengthen the resilience of the digital infrastructure in low and middle-income countries. This Multi-Donor Trust Fund aims to better define, understand, articulate, structure, and rollout the cybersecurity development agenda in a systematic manner. The program offers comprehensive cybersecurity capacity development, including development of global knowledge, country assessments, technical assistance, capacity building and training, underpinned with necessary investments in infrastructure and technology.

Germany's vision of the UN's role in the cybersecurity landscape

Ultimately, Germany believes that this mapping exercise and the future role of the UN in CCB should contribute to ensuring everyone has a seat at the table in the facilitation of capacity-building efforts to complement the extensive amount of already existing offers in this regard such as coordination efforts already undertaken by the Global Forum on Cyber Expertise (GFCE).

Building on this, Germany is convinced that the envisaged UN Program of Action would serve as a powerful practical mechanism to facilitate access to cyber capacity building solutions for UN member states while respecting the already agreed upon UN principles. Moreover, we are convinced that incorporating more women into cyber can only be ensured via mainstreaming gender activities into all cyber capacity building efforts. Finally yet importantly, Germany believes UN's mapping exercise and follow-up activities can be detrimental in providing further guidance on to link the cyber and development community and more specifically, how cyber capacity building can contribute to the delivery of the Sustainable Development Goals in line with the recent Global Conference on Cyber Capacity Building (GC3B) in Accra.