# Contribution by the Global Forum on Cyber Expertise (GFCE) Foundation Board

*Tuesday 12 December 2023*

The GFCE is an apolitical multistakeholder community of more than 200 members and partners including member states, international and regional organizations, and actors from the private sector, civil society and academia. It is dedicated to the global coordination and promotion of cyber capacity building.

## The Accra Call for Cyber Resilient Development: An Action Framework

As Member States meet for the sixth substantive session of the Open-ended Working Group on security of and in the use of information and communications technologies (2021–2025), the GFCE Foundation Board would like to highlight the recent launch of the **Accra Call for Cyber Resilient Development: An Action Framework**, an outcome document of the inaugural Global Conference on Cyber Capacity Building (GC3B) that took place from 29-30 November 2023 in Accra, Ghana.

The goal of the Accra Call is to stimulate global action to elevate cyber resilience across international and national development agendas, as well as to promote cyber capacity building that supports broader development goals, effectively (and especially) serving the needs and priorities of developing countries.

At the time of writing, the Accra Call has been endorsed by 44 signatories – 16 UN Member States and 28 other stakeholders (including international organisations such as UNODC, Interpol, the African Union, and the European Union) – and continues to welcome further endorsements from States and organisations that wish to affirm the principles and commitments of the Call.

The Accra Call draws on existing shared commitments and ongoing relevant efforts in international fora and processes. It serves as both a blueprint and a motivation for voluntary action to:

- Strengthen the role of cyber resilience as an enabler for sustainable development;
- Advance demand-driven, effective, and sustainable cyber capacity building;
- Foster stronger partnerships and better coordination; and
- Unlock financial resources and implementation modalities for cyber resilience.

These four thematic areas are further broken out into 16 key Actions, which form the Action Framework.

The GFCE, as a trusted, neutral convenor for the global cyber capacity building community, will shepherd a process to build on this starting point. This includes fostering an active multistakeholder community of those that have endorsed the Accra Call or pledged voluntary commitments related to any of the specific Actions, sharing insights on lessons, successes, and challenges that will inform the collective follow-up and subsequent iterations of the Accra Call.

## From Words to Actions: the GC3B

As noted above, the Accra Call is an outcome document of the inaugural **Global Conference on Cyber Capacity Building (GC3B)** that took place from 29-30 November 2023 in Accra, Ghana.

Responding to the rapid pace of technological development (including in the field of artificial intelligence, which has now fully entered the public space) and the evolving demands and risks of digitalization, the GFCE took the initiative, along with partners including the World Bank, the World Economic Forum, the CyberPeace Institute and our host, the government of Ghana, to organise a unique conference that gathered around 800 high-level leaders, experts on cyber security and capacity building, and the international development community to work together on common goals and solutions.

Participants at the GC3B met with an overarching goal: to catalyse global action to elevate cyber resilience across international and national development agendas. Recognising that cyber resilience is a key enabler of sustainable development, inclusive economic growth, and social prosperity for all, the GC3B was an opportunity to discuss the practical commitments that will be required from all stakeholders if this ambition is to become a reality.

The Accra Call represents a significant, concrete step in identifying and working towards those commitments.

Likewise, the announcement during the conference of a new effort integrating data from the GFCE's **Cybil Knowledge Portal** (which contains information on around 900 cyber capacity projects and over 300 tools and resources) on UNIDIR's Cyber Policy Portal. This initiative, which will be officially launched during the OEWG's sixth substantive session in New York, represents an important practical step to ensure that all stakeholders can more easily access the knowledge, experience, and resources that are available via these platforms, and which are essential to effective cyber capacity building.

This kind of cooperation between the GFCE and UNIDIR is an example of the Accra Call Action 12, which urges stakeholders to, "Utilize existing platforms to better coordinate and deconflict cyber capacity building financing and actions" (Action #12), a goal that strongly aligns with the outcomes of earlier OEWG discussions.

## Next Steps

Building cyber capacity is an inclusive and iterative process: a key dimension of the Accra Call will be to facilitate stakeholders learning from each other and leveraging each other's strengths and capabilities.

It was announced as part of the GC3B in Accra that the next GC3B meeting will be held in Geneva in May 2025, with a goal of building on the progress initiated in Ghana. All Member States and other stakeholders in the OEWG discussions are warmly invited to participate in this event.

Likewise, all Member States and other stakeholders are encouraged to consider supporting the Accra Call, either by endorsement (expressing non-binding, voluntary, public support for the Accra Call's objectives) or by pledging voluntary commitments in relation to any of the Accra Call Actions. Those who have endorsed the Accra Call or made specific pledges will be invited to share their experiences in pursuit of the Call's actions, and these insights will inform the collective follow-up on the Accra Call at the next GC3B in 2025.

The full text of the Accra Call for Cyber Resilient Development can be found in Annex or online here: https://gc3b.org/the-accra-call-for-cyber-resilient-development/.

All stakeholders wishing to affirm their willingness to promote, pursue, and coordinate efforts on the Accra Call through endorsement and/or through pledges can do so via the webform at: https://gc3b.org/support-the-accra-call/

The GFCE Foundation Board wishes participants in the sixth substantive session of the Open-ended Working Group on security of and in the use of information and communications technologies (2021–2025) a productive meeting.

# ACCRA CALL FOR CYBER RESILIENT DEVELOPMENT

## AN ACTION FRAMEWORK

GC3B

Global Conference on Cyber Capacity Building

# BACKGROUND

The widespread adoption of digital technologies and services has driven economic growth, human and social development, and has the potential to significantly advance the goals of the 2030 Agenda for Sustainable Development and the Addis Ababa Action Agenda.

The rapid expansion of digitalization and connectivity has also created new demands on resources, expertise, and skills necessary to reap the digital dividends and manage related risks and challenges. As cybersecurity vulnerabilities and threats continue to grow in volume, scope, and sophistication, they can stifle growth, weaken the resilience of critical infrastructure, erode trust in the digital environment, and endanger the lives, health, well-being, and public participation of people.

The capacity to anticipate and withstand such threats, promote the rule of law and uphold human rights, as well as maintain societal trust in the use of digital technology, is central to the delivery of key development outcomes and achieving the Sustainable Development Goals. Yet, the persistent digital divides, inequalities in acquiring digital skills, and uneven access to cybersecurity expertise and resources – that affect particularly developing countries – undermine efforts to implement the 2030 Agenda and 'leave no one behind'.

Demand for cyber capacity building, particularly among developing countries, is both strong and increasing – far outstripping the current supply of such assistance. While international cooperation efforts have expanded over time to enhance the cyber resilience and preparedness of developing countries as well as their capacity to address cybercrime, cyber capacity building has not necessarily been a priority for decision makers globally. These efforts have also been slow to systematically embrace and link to the larger development agenda. This has resulted in limited financial allocations, ad hoc implementation approaches, and fragmented coordination efforts that hinder the impact of relevant national, regional, and international initiatives.

We are at an inflection point, as investments in digital infrastructure, systems, and services are accelerating across the world, while development approaches are also increasingly relying on digital tools and solutions for service delivery. This calls for greater integration of cyber capacity building and traditional development programs – including incorporating cyber resilience across national and international development investments and projects to help ensure the viability and sustainability of development results in the face of growing cyber threats.

On the occasion of the 2023 **Global Conference on Cyber Capacity Building** in Accra, Ghana, and drawing from existing shared commitments and ongoing relevant efforts in international fora and processes, the Accra Call for Cyber Resilient Development aims to stimulate action and voluntary commitments to elevate cyber resilience across international and national development agendas as well as promote cyber capacity building that supports broader development goals and effectively serves the needs and priorities of developing countries.

Accordingly, governments, development donors and partners, multilateral and bilateral financial institutions, international and regional organizations, the private sector, the technical community, civil society, academia, and philanthropic institutions, within their respective mandates, affirm their willingness to promote, pursue, and coordinate efforts on the following voluntary actions:

# STRENGTHEN THE ROLE OF CYBER RESILIENCE AS AN ENABLER FOR SUSTAINABLE DEVELOPMENT

*Cyber resilience can play a crucial role in achieving sustainable development objectives, managing risk in national and international development investments, promoting the rule of law, contributing to international security and stability, and protecting and realizing human rights. Key actions to consolidate this multi-faceted role include:*

1. Encourage decision-makers across different strategic areas, including development, security, technology, and diplomacy, to integrate cyber resilience into national, regional, and international sustainable development strategies as a cross-cutting priority.

2. Promote the mainstreaming of cyber resilience across international development programming, including the roll-out of digital risk impact assessments in the design of initiatives, accompanied by digital risk mitigation and management plans during implementation.

3. Accelerate the integration of the cyber capacity building community of practice with the development field to consolidate its links and approaches with broader development goals. This can be pursued, inter alia, by creating opportunities for more structured dialogues involving the respective communities, leveraging the convening power of existing multistakeholder platforms.

4. Strengthen and promote cyber resilience knowledge and skills among international development workforce – including donors, implementors, and partner organizations – through the development and implementation of regular training and education courses.

# ADVANCE DEMAND-DRIVEN, EFFECTIVE, AND SUSTAINABLE CYBER CAPACITY BUILDING

*Cyber capacity building efforts to date highlight the need to tailor investments and efforts to the financial, institutional, technical, and human capabilities of developing countries and address all segments of society to foster effective, inclusive, and locally sustained change. Key actions include:*

5

Design and implement cyber capacity building initiatives that tackle both existing and emerging gaps across policy, technology, legal, regulatory, and institutional frameworks with activities customized to each country's and region's unique context and absorption capacity.

6

Invest in capacity building that enhances the cyber resilience of significant sectors in the economy and in public service delivery (such as essential services, critical infrastructure, as well as infrastructure that is critical to the availability and integrity of the internet), promotes a holistic risk management approach, and increases opportunities to prosecute and adjudicate cybercrime.

7

Ensure that all cyber capacity building investments and programs take into account the prevalent cybersecurity skills gap and its gendered dimension and adapt as necessary to include relevant and context-based education, skilling, reskilling, and upskilling activities, components or stand-alone initiatives that are sensitive to the needs of women and girls, the youth, persons with disabilities, rural and remote communities, vulnerable and marginalized groups.

# ADVANCE DEMAND-DRIVEN, EFFECTIVE, AND SUSTAINABLE CYBER CAPACITY BUILDING

8

Commit to further professionalize the cyber capacity building community of practice. This includes developing practical tools and guides that can help stakeholders put into practice established principles, notably those defined in the 2017 Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building, the 2021 consensus report of the UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, and the Global Partnership for Effective Development Cooperation.[1]

9

Accelerate efforts to improve the measurement of cyber capacity building results. This can be achieved by actively and systematically integrating methodologies and good practices from the international development field, such as: leveraging nationally-led statistical and monitoring mechanisms in developing countries to strengthen their data collection, metrics, and monitoring capacities in the field of cybersecurity; systematizing project monitoring and evaluation frameworks; as well as ensuring that cyber capacity building programming is adaptable to the findings of evaluation processes.

[1] For instance, such tools and guides could offer practical guidance on how to integrate results-oriented, human rights-based, gender-responsive and inclusion-sensitive approaches across cyber capacity building strategies, project cycles, and processes.

# FOSTER STRONGER PARTNERSHIPS AND BETTER COORDINATION

*The cross-sectoral and interdependent nature of cyber resilience also necessitates whole-of-society and whole-of-ecosystem approaches to cyber capacity building that promote effective multistakeholder partnerships, leverage the value added that the private sector, the technical community, and civil society bring in terms of expertise and investment, and enable effective coordination within national, regional and international levels. Key actions include:*

10

Foster the leadership of developing countries in coordinating cyber capacity building efforts in close cooperation with donor governments and organizations, Development Finance Institutions, the private sector, and other multistakeholder community partners, as a means to promote ownership of initiatives, effective use of limited resources, improved transparency, as well as better division of labor amongst donors and development partners.

11

Promote public-private partnerships as well as inclusive and equitable market incentives to enhance cyber resilience in developing economies. This includes supporting the creation and development of local cybersecurity markets and ecosystems to foster home-grown cybersecurity talent and services that can accelerate a secure digital transition as well as contribute to the expansion of the local economy and create decent, high-value jobs

# FOSTER STRONGER PARTNERSHIPS AND BETTER COORDINATION

12

Utilize existing platforms to better coordinate and deconflict cyber capacity building financing and actions. This includes supporting the role of regional organizations and regional hubs in improving awareness and coordination of cyber capacity building efforts to curb duplication, leveraging the value added and efficiencies that regional coordination approaches can have in bridging national and international levels. Examples include the Global Forum on Cyber Expertise and its regional hubs for Africa, the Americas, the Pacific and Southeast Asia.

13

Encourage greater information sharing and relationship building between the cybersecurity community and development stakeholders – including donors, implementing organizations, and local partners – on cyber threats, incident response, and remediation. This can be pursued through existing regional or international bodies, or for example through new mechanisms such as Information Sharing and Analysis Centers (ISACs) for development stakeholders.

# UNLOCK FINANCIAL RESOURCES AND IMPLEMENTATION MODALITIES

*The growing need for integrating cyber resilience across development approaches – against competing priorities and financial limitations – requires the deliberate deployment of all available financing options and implementation modalities. Key actions include:*

14

Encourage developing countries to work closely with donor governments and organizations, Development Finance Institutions, and development partners – including private sector and philanthropic institutions – to identify and employ the full range of financial streams available to weave sustainability into the financing of national cyber resilience activities, and design for financial and development additionality. This entails a meaningful combination of international development financing, domestic resource mobilization, private sector investments, and the incorporation of cyber resilience in Integrated National Financing Frameworks.

15

Diversify program implementation modalities used to support developing countries in strengthening their cyber resilience capabilities, and utilize all available options – from technical assistance, grants, budget support, blended finance, and loans – after assessing the most effective approach for meeting national needs and alleviating structural barriers to local actors' access to funding.

16

Systematize South-South and Triangular cooperation in cyber capacity building actions to enable cost-effective and context-sensitive interventions between partners with similar cyber resilience paths and to empower more countries to join global cyber resilience efforts.

All stakeholders are invited to endorse the Accra Call for Cyber Resilient Development and are encouraged to make voluntary commitments or pledges on their plans to implement it. Progress in the realization of the Action Framework of the Accra Call for Cyber Resilient Development and any needed update will be reviewed every 2 years at the next iterations of the Global Conference on Cyber Capacity Building. This process will be led by the Global Forum on Cyber Expertise.

Interested in learning more about the Accra Call and supporting it through endorsements or pledges?

Scan the QR code to access the webpage for more information, as well as to learn more about those who have committed their support. For more information, please email contact@gc3b.org.

GC3B Global Conference on Cyber Capacity Building