PRESS RELEASE

Global Conference on Cyber Capacity Building results in action framework for cyber resilient development

Governments and organizations from across the globe endorse the Accra Call

Accra, 29 November 2023 – Today, at the first Global Conference on Cyber Capacity Building (GC3B), the Accra Call was announced. In this international action framework governments and many organizations across all sectors and regions affirm their willingness to voluntarily promote, pursue and coordinate efforts on sixteen specific actions to elevate cyber resilience across international and national development agendas. In addition, the actions in the framework aim at promoting cyber capacity building which supports broader development goals and effectively serves the needs of developing countries.

Photo: Senior Presidential Advisor H.E. Yaw Osafo-Maafo signs the Accra Call, in presence of Honourable Minister of Communications and Digitalisation Ursula Owusu-Ekuful and Director-General of the Cyber Security Authority, Dr. Albert Antwi-Boasiako

Cyber capacity building as a key enabler for sustainable development, growth, and progress

The Global Conference on Cyber Capacity Building (GC3B) was organized to raise awareness of the importance that every nation has the expertise, knowledge, and skills to invest in their digital future, and to encourage countries to work together on developing these capabilities to ensure a free, open, and secure digital world. For the first time, high-level leaders, experts on cyber security and capacity building, and the international development community from around the world were brought together to work on common goals and solutions. The GC3B also addressed the international need to increase resources for cyber capacity building, which is a key enabler for sustainable development, economic growth, and social progress. The announcement of the Accra Call was the highlight of the conference.

Endorsers of the Accra Call

The following governments and organizations from all over the world endorse the Accra Call.

- Microsoft
- European Union (EEAS)
- ValU
- Interpol
- UK
- Global Partners Digital
- GFCE
- CyberPeace Institute
- Forum of Incident Response and Security Teams, Inc. (FIRST)
- CREST
- Africa Youth Forum International
- Tonga Computer Emergency Response Team (CERT Tonga)
- Orizur Consulting Enterprise Pty Ltd
- Government of The Netherlands (Ministry of Foreign Affairs)
- Government of the Republic of North Macedonia
- Royal Holloway University of London
- BAE Systems Digital Intelligence
- Switzerland
- Cyber Intelligence And Security Aid Bureau - CISAB
- Neurometrics
- Mexico - Ministry of Foreign Affairs
- France
- Word of Life Permanent Mission Office to the United Nations (Office of the Special Envoy to Government)
- Global Cyber Alliance
- Republic of Slovenia
- ESET
- West Africa ICT Action Network

- Austria
- African Telecommunications Union (ATU)
- Sweden
- The Shadowserver Foundation
- NetHope
- IST
- ICC
- Canada
- African Union – David
- Estonia Ministry of Foreign Affairs

Cyber resilience is critical for the digital transition

The digital world touches every aspect of our lives. It enables us to connect, work, learn and travel, and plays an important role in safeguarding life essentials, such as food, water, and healthcare. Along with huge opportunities, this also comes with digital risks. We need to be aware of those risks - all of us. Governments. Businesses. Academia. Society at large. To ensure a free, open, and secure digital world, every country should have the resources, knowledge, and skills they need to invest in their digital future. Nations should work together and support each other with these capabilities, so that no country is left behind in their digital evolution. After all, a chain is only as strong as the weakest link.

The sixteen actions of the Accra Call

The Accra Call is endorsed by 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. The action framework consists of sixteen actions, divided in four categories:

- *Strengthening the role of cyber resilience as an enabler for sustainable development*: cyber resilience can play a crucial role in achieving sustainable development objectives, managing risks in national and international development investments, and contributing to international security and stability.
- *Advancing demand-driven, effective, and sustainable cyber capacity building*: cyber capacity building experience to date highlights 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.
- *Fostering 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 meaningful 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.
- *Unlocking financial resources, cooperation, and implementation modalities*: The growing need for integrating cyber resilience across development approaches along with the increased demand by developing countries for cyber capacity building – against existing multiple priorities and financial limitations – require the deliberate deployment of all available financing options, cooperation, and implementation modalities beyond what has been traditionally done to date.

By promoting, pursuing, and coordinating efforts on these actions, cyber resilience will be elevated across international and national development agendas, and cyber capacity building will be promoted to support broader development goals and effectively serve the needs of developing countries.

Looking ahead – evaluating actions in 2025

Progress of these actions will be reviewed every two years at the next iterations of the Global Conference on Cyber Capacity Building, led by the Global Forum on Cyber Expertise. The next GC3B is scheduled for 2025 and will be hosted by the government of Switzerland.

About the GC3B

The Global Conference on Cyber Capacity Building is co-organized by the Global Forum on Cyber Expertise, the World Bank, the Cyber Peace Forum, and the World Economic Forum, and hosted by the government of Ghana.

Additional information:

- Please find herewith the full Accra Call