GC3B Global Conference on Cyber Capacity Building

ACCRA CALL FOR CYBER RESILIENT DEVELOPMENT

THE ROAD TO GENEVA: NOTES FROM A TRAVEL JOURNAL

OUTCOME DOCUMENT OF GC3B 2025

Table of Contents

Authors: Patryk Pawlak and Nayia Barmpaliou, GC3B Advisors

May 2025

Disclaimer: The conclusions in this document build on authors' own assessment based on interviews with endorsers and pledgers as well as on the results of a survey conducted in March-April 2025. They do not necessarily represent the views of the Global Conference on Cyber Capacity Building (GC3B) hosts, the Global Forum on Cyber Expertise, or any of its members and partners.

The Journey Begins

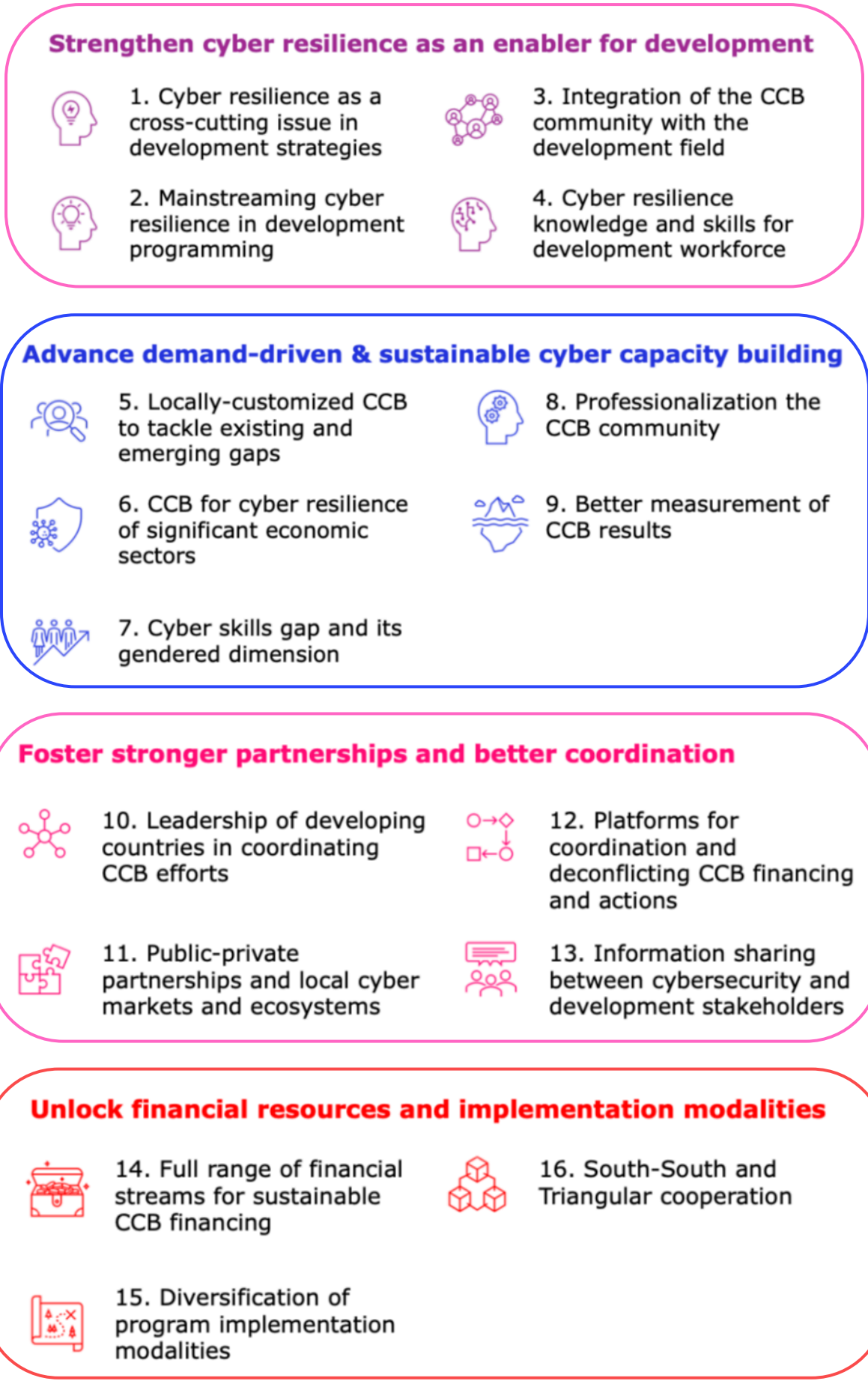
The Accra Call for Cyber Resilient Development ("Accra Call") was endorsed by nearly 80 countries and organization at the first Global Conference on Cyber Capacity Building (GC3B) hosted by Ghana in 2023. The Accra Call provides a blueprint to mainstream global action for cyber resilient development. Building on the achievements of the GFCE Delhi Communique on Capacity Building, the document responded to the urgent need for a sense of direction and to set priorities for the expanding cyber capacity building ecosystem. In that sense, the Accra Call responded to the key trends identified by research, including the growing fragmentation in cyber capacity building, the gap between the ambitions for and realities in coordination, or the slow convergence of different communities of practice working on cyber capacity building .

In Accra, further to the endorsers, about 20 organizations also recognized the immediate value of the Accra Call and were inspired to use it as a map to navigate their cyber capacity building journey. The specific pledges made as a result range from the commitment to support closing the cyber skills gap and supporting work to professionalize the cybersecurity community, to organizing cyber awareness programs for youth and entrepreneurs, and operationalizing and scaling the Global Humanitarian ISAC, among others, with key highlights captured in a series of **Accra Call Action Stories**.

Reflecting on the process to date, this report takes stock of the progress in achieving of the Accra Call actions and pledges and to provide an **overview of lessons and practices ("travel notes") that may be useful for the broader cyber capacity building community in turning the Accra Call into an operational roadmap to inspire further actions.** The selected travel notes presented in this report address both the output, i.e., *how the Accra Call has inspired the community*, and input dimensions, i.e., *how the Accra Call needs to adapt to the evolving policy and operational environment*.

The conclusions of the report are two-fold. First, in reference to specific actions and priorities, the Accra Call should be a dynamic and evolving document. Whereas **the Accra Call provides overall orientation as to the direction of travel, the cyber capacity building community may choose to prioritize different aspects at different points in time**. For instance, in 2023 the primary preoccupation of the endorsers was bridging the gaps between cyber and development communities. In 2025, there is also a strong interest in finding more sustainable, scalable and innovative ways for financing the delivery of cyber capacity building projects.

Figure 1. The Accra Call for Cyber Resilient Development



Second, regarding the process, **the progress on the Accra Call pledges was possible primarily thanks to grassroot initiatives driven by specific pledgers and endorsers without a coordinated process**. While this allowed for multiple initiatives to flourish, it also demonstrated that **the field of cyber capacity building continues to be driven and shaped by a small number of policy entrepreneurs.** Whereas the community seems to be expanding in the number and scope of issues that it addresses, the efforts remain largely fragmented between different initiatives, which also undermines the sense of community and a shared destination of travel.

Looking into the future, the report reiterates **the need for a process that will enable and propel closer and more systematic dialogue between development, digital transformation, cybersecurity and financial development communities at various junctures** between the GC3B conferences. It points to the need for an Accra Call process that provides a space for action-oriented dialogue between these critical stakeholder groups outside of traditional conference formats. In relation to that, the report makes also two specific recommendations for the GC3B community supported by the Global Forum on Cyber Expertise (GFCE): to develop a Roadmap for a Resilient Digital Transformation Financing Scheme, and to establish a Resilient Digital Transformation Alliance.

The conclusions in this report are based on the authors' assessments based on interviews with endorsers and pledgers as well as on the results of a survey conducted in March-April 2025. They do not necessarily represent the views of the Global Conference on Cyber Capacity Building (GC3B) hosts, the Global Forum on Cyber Expertise, or any of its members and partners.

Figure 2. The Accra Call for Cyber Resilient Development:

A Travel Map

Note 1: Accra Call serves to motivate, validate and accelerate action

The Accra Call has served as a catalyst to motivate, validate and accelerate actions. For several organizations active in or entering the field of cyber capacity building, the Accra Call has provided a narrative, guidance and a source of internal validation for the ongoing or planned processes and initiatives.

In France, the Accra Call was an important factor in **prompting a more strategic reflection internally on the role of cyber capacity building in their broader cyber policy frameworks**. This led France shape its strategic approach to cyber capacity building, including their programming priorities, in alignment with the Accra Call to establish itself as "a responsible, cooperative power acting in solidarity in cyberspace". For instance, the Accra Call actions promoting closer coordination between different actors was an important element in the design and operationalization of the Western Balkans Cyber Capacity Centre (WB3C) founded by France and Slovenia in Montenegro. To ensure more local ownership and cooperative approaches, the WB3C was established as an international organization with a truly inclusive governance to make sure it is a demand-driven platform where the voices of beneficiary countries are at the same level as those of donor countries.

The Accra Call has also served to accelerate planned initiatives. NetHope, in collaboration with is members and partners, have committed to operationalize and scale the Global Humanitarian Information Sharing and Analysis Centre (GH ISAC), as a shared digital public good. Through the GH ISAC the community pledged to provide a shared platform run for and by the international nonprofit community to enable intelligence-led approaches, to build knowledge and resilience through peer learning, to foster equitable collaboration, convening, and skills-development for underserved communities, as well as to facilitate the rapid increase of their uptake of private and public sector-led capacity building. Since Accra, NetHope has developed partnerships critical for this goal, including with CISCO, OCTA, SANA and NGO-ISAC.

The Accra Call has also **enabled its supporters to demonstrate to the world their commitment to cyber capacity building, often facilitating new connections or partnerships**. For example, the Shadowserver Foundation, nonprofit security organization, used its pledge to reiterate its mission to improving cyber resilience globally by providing free cyber threat intelligence to National CSIRTs and network owners. While not a new initiative, the framework of the Accra Call has supported the Shadowserver Foundations' engagement with donors as it underlined its commitment to cyber capacity building efforts.

Note 2: Accra Call serves to inspire new initiatives

The Accra Call has inspired the cyber capacity building community to take new initiatives or provide direction to the ongoing processes. While there is limited evidence to demonstrate that the Accra Call is the reason for many new initiatives, it has certainly enriched the design of new actions and influenced the implementation of ongoing processes and initiatives.

As one of the first endorsers, the International Chamber of Commerce (ICC) drew inspiration from the Accra Call to **support whole-of-society and whole-of-ecosystem approaches in cyber capacity building.** Since then, the ICC has worked more systematically to identify ways in which the private sector expertise and experiences can be featured more effectively in the government thinking and planning around cybersecurity and cyber resilience. One of the highlights in this effort is the release of a report on protecting cybersecurity of critical infrastructures and their supply chains. Instead of adopting a fragmented approach with the focus on technical issues, the report takes inspiration from the Accra Call to promote the whole-of-ecosystem approach with recommendations addressed to governments, businesses and public-private partnerships and ultimately strengthen a more holistic thinking on these issues.

Similarly, the Accra Call was instrumental in helping shape CREST International's **strategic thinking on designing and developing a cyber capacity building offering** within CREST's mandate and product range as an international not-for-profit, membership body representing the global cyber security industry. CREST's pledge in Accra focused on a 50% discount on all CREST products for applicants from low and low middle income countries – which they have implemented but, most significantly, other actions in the Accra Call framework informed the development of their CREST Camp initiative to supporting local ecosystems of cybersecurity service and training providers at lower levels of maturity to become aspirant CREST members through mentorship and capacity-building.

The Accra Call has also **inspired adjacent ongoing processes to integrate cyber capacity building into a set of broader issues**. The Pall Mall Process launched by the United Kingdom and France in February 2024 to tackle proliferation and irresponsible use of commercial cyber intrusion capabilities has gradually embraced cyber capacity building as one of the main aspects in the Code of Practice for States presented in April

2025. This non-binding set of guidelines puts particular importance to cyber capacity building across four guiding pillars of the Code: accountability, precision, oversight and transparency. The Code of Practice also reflects the spirit of the Accra Call in that it attempts to match foreign policy objectives in cyber policy with the legitimate interests of developing countries to acquire certain tools for defensive purposes that would allow them to protect their developmental goals.

Note 3: Accra Call is driven by a bottom-up approach

Without any centralized coordination mechanism, the Accra Call has been kept alive by the selected members of the cyber capacity building community who acted as curators and custodians of the principles and actions that inspired the Accra Call.

The relevance of the Accra Call has been assured by a community of practice formed by governments, private sector and civil society organizations that recognized the benefits of the Accra Call for their own organizations. **Even where no explicit link to the Accra Call is acknowledged, the initiatives that align with the Accra Call spirit provide a valuable validation mechanism**.

In India, the Digital Empowerment Foundation (DEF) mobilized resources for the **implementation of projects that converge with the goals of the Accra Call, indirectly providing validity for specific Accra Call actions**. The DEF's main focus is to make technology easily accessible and to empower women, youth, persons with disabilities, and the elderly through providing functional digital literacy, media literacy, and digital up-skilling across agriculture, micro and nano-business, health, education, livelihood, and entrepreneurial skills. In over two decades of its activities, DEF has created 2000 Community Information Resource Centres that are supported by a widespread network of 10,000 digital foot soldiers located across 25 states and 250+ districts in rural, tribal, marginalized, and unreached areas. By providing locally-driven and context-specific support, the programmes and initiatives by EDF may serve as a source of inspiration for other regions.

Another example is the work of the Cyberplace Institute (CPI) that endorsed the Accra Call to **reflect its commitment to responsible cybersecurity**. The Accra Call served as a catalyst to expanding CPI's support to civil society, including through accelerating skills development and deepening cross-sector collaboration. While many CPI initiatives – such as the Cyberplace Builders and the CyberPeace Academy – have not been conceived with the Accra Call framework in mind, their focus to vulnerable communities on the ground offering context-specific cybersecurity skills and threat intelligence support to more than 400 NGOs to foster their capacities to across the world fully aligns with the Accra Call ethos for addressing the prevalent cybersecurity skills gap in ways that are sensitive to the needs of different stakeholders' needs, including vulnerable groups.

NOTE 4: ACCRA CALL NEEDS TO BE A DYNAMIC INSTRUMENT

The Accra Call actions have provided an impetus and a direction necessary to the approach and prioritization of cyber capacity building engagements. However, against the growing needs and constraints on resources, the priorities will be shifting over time. For the Accra Call to remain a relevant framework, it is critical to ensure that it is a dynamic document.

The Accra Call as a framework to guide actions of the cyber capacity building community was developed through consultations mainly with the GFCE community. The outcome of this process is contained in a catalogue of 16 actions which the community found to be the most relevant. As part of the follow-up process, individual organizations and institutions could decide which of the actions they wish to prioritize through their own engagements. While some have made concrete pledges, others implicitly aligned their activities with the Accra Call actions.

Given the voluntary nature of the framework and the reluctance of stakeholders to include a structured monitoring system to the Accra Call at the time of its negotiation, it is difficult to assess which specific actions have been prioritized as well as who and to what extent takes up individual Accra Call actions or contributes towards the framework's overall vision.

The analysis of the 2023 pledges and information collected through interviews and consultations with individual pledgers and endorsers of the Accra Call, as well as a review of projects in the Cybil Portal active during this period, suggest that **the community has embraced in particular the following actions**:

- **Action 1:** Encourage decision-makers across different strategic areas to integrate cyber resilience into national, regional, and international sustainable development strategies.
- **Action 2:** Promote the mainstreaming of cyber resilience across international development programming.
- **Action 5:** Design and implement cyber capacity building initiatives that tackle both existing and emerging gaps across policy, technology, legal, regulatory, and institutional frameworks.

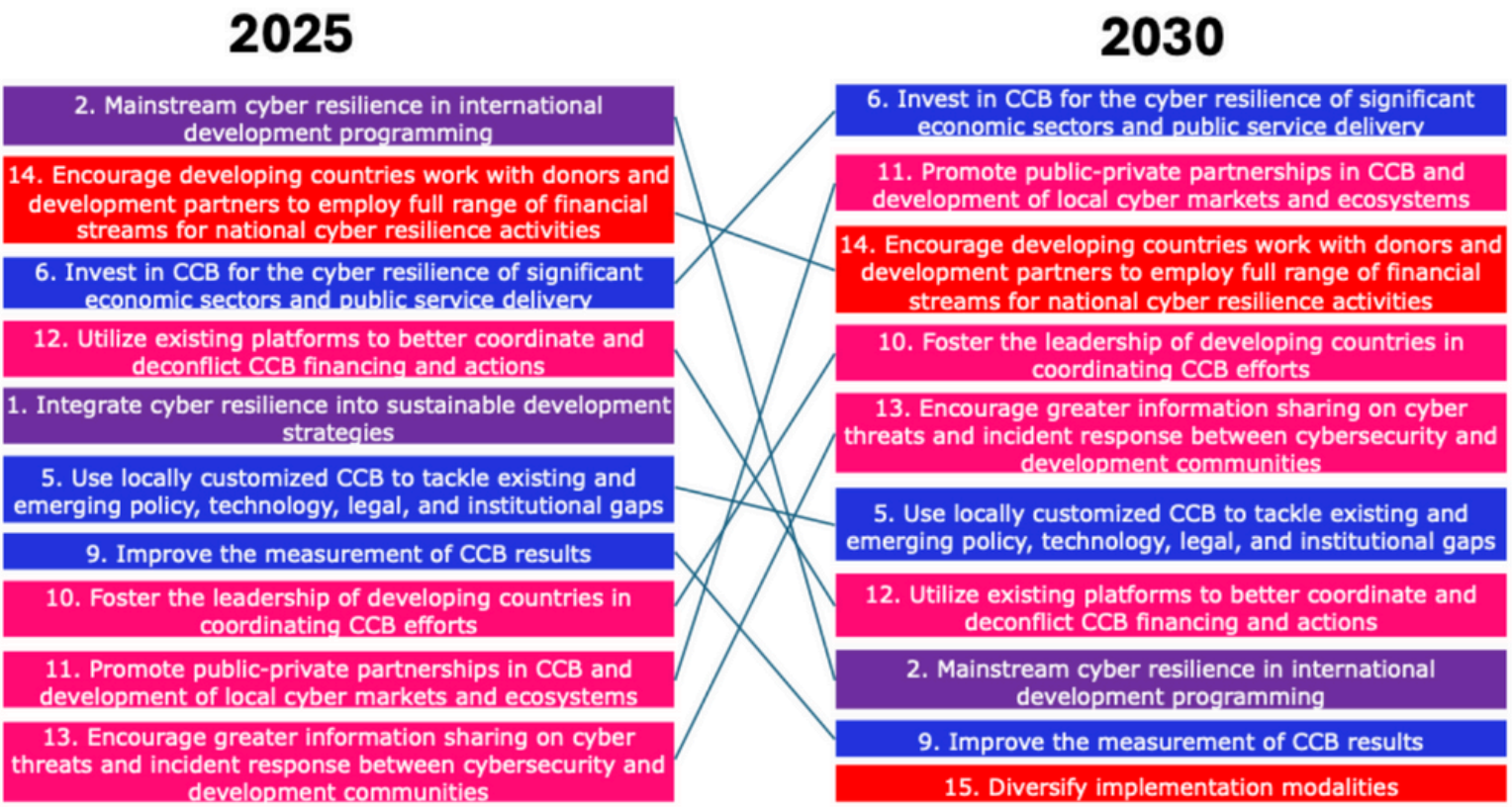
- **Action 7:** Ensure that all cyber capacity building investments and programs take into account the prevalent cybersecurity skills gap and its gendered dimension.
- **Action 8:** Commit to further professionalize the cyber capacity building community of practice.
- **Action 11:** Promote public-private partnerships as well as inclusive and equitable market incentives to enhance cyber resilience in developing economies.
- **Action 13:** Encourage greater information sharing and relationship building between the cybersecurity community and development stakeholders on cyber threats, incident response, and remediation.

A sample of very limited results from a survey distributed to the Accra Call supporters and the GFCE community in March 2025, along with the interviews conducted with Accra Call supporters, suggest that actions identified in 2023 evolved both in terms of content and priority. When asked about which Accra Call actions are the priority in 2025, the respondents have identified mainstreaming cyber resilience in international development programming as a top priority. Strengthening cyber resilience as an enabler of development dominates the list of top 5 priorities.

However, the respondents have a different **outlook for the situation in 2030**. Integration of cyber resilience into sustainable development strategies is no longer in the top 10, while diversification of implementation modalities appears as the new top priority for the next five years. The top 5 list is dominated by actions aimed at fostering stronger partnerships and better coordination.

Given the size of the sample, these results need to be read with caution. However, the likely adjustments of priorities suggests that there will be a need to put in place mechanisms with the support of the GFCE that will foster collective reflections on these issues and catalyze action that is responsive to these evolving priorities.

Figure 3. Perception of the top 10 Accra Call action priorities: 2025 & 2030



Source: Based on a sample of 15 responses from a GC3B survey

NOTE 5: THE ACCRA CALL SHOULD BE A SHARED RESPONSIBILITY.

Despite a broad number of endorsers and pledgers, the Accra Call vision continues to be driven by a small number of stakeholders, primarily from the private sectors and civil society organizations. A more robust whole-of-ecosystem approach is needed to deliver a more sustainable and impactful community on the Accra Call.

Two years since the adoption of the Accra Call, the number of the endorsers has increased from 50 to 80, yet new, additional pledges have not been made since – even though many supporters have been referencing the value of the Accra Call in different fora and have launched new cyber capacity building initiatives that align with its actions. Moreover, the rather low number of responders to the Accra Call survey and a small group of organizations that was ready to share their experience in how the Accra Call informed their work, would suggest that **a more systematic effort is needed in keeping the community of the Accra Call supporters engaged and further expanding it and possibly better connecting it with the GFCE processes as the latter is bestowed with leading the review of the Accra Call.**

Several Accra Call pledgers have confirmed that while the community acknowledges that cybersecurity is a shared responsibility, the exact implications of such approach differ between stakeholder groups. For governments, for instance, this may mean simply delegating certain responsibilities to operators and the private sector without involving them in early stages of designing specific measures. The lack of a more inclusive and structured approach to distribution of different responsibilities often leads to a “buck passing” mentality, avoidance of responsibility and ultimately accountability vacuum. This is particularly relevant in the context of countries with a significant presence of small and medium-sized companies that often do not have sufficient resources to meet obligations imposed on them. **Designing an incentive structure that makes collaboration and joint goal setting a priority emerged as one potential solution.**

NEXT DESTINATION: FROM A FRAMEWORK TO A PROCESS

Looking into the future, the report reiterates the need for conversation between development, digital transformation, cybersecurity and financial development communities. It points to the need for **an Accra Call process that would provide a space for action-oriented dialogue between these critical stakeholder groups outside of traditional conference formats**. The future success of the Accra Call as a framework to guide cyber capacity building actions will depend on two aspects.

First, governments to fulfil their responsibility for their own economic and social development – as defined in the 2030 Agenda for Sustainable Development – largely depends on the **effective mobilization of all possible financing streams**. International cooperation efforts for cyber resilient digital development to date have focused on a patchwork of technical assistance, grants, ad-hoc public-private partnerships, and the gradual expansion to development loans, that are not designed for sustainable impact. **A key solution lies with weaving sustainability into the financing of digital and cyber resilience development and meaningfully considering the systematic partnerships required to deliver it**. To achieve that, the GFCE community should consider leveraging the GC3B platform:

1. To develop a **Roadmap for a Resilient Digital Transformation Financing Scheme** (a concept for a financing solution): Such concept would contain a list of recommendations regarding ways to streamline and improve financing for cyber and digital capacity building to respond more efficiently to the needs of the Global Majority countries and be adaptive to the major ongoing transformation of the international cooperation financing landscape. The development of such a concept is fully aligned with the Accra Call pillar that calls for unlocking financial resources and implementation modalities and would support the community also identify investment-driven models that prioritize mutual benefit as an addition to traditional models used to date in cyber capacity building.

1. To establish a **Resilient Digital Transformation Alliance** (a partnerships solution): A footprint for such Alliance will provide a framework of how an effective cooperation mechanism between different stakeholders could look to deliver on the recommendations presented in the Roadmap. The Alliance would be

multistakeholder in nature and bring together representatives of Development Finance Institutions, governments, national development agencies, the private sector, technical experts, and other communities. Considering the existing footprint of its established community and its role as the custodian of the Accra Call, the GFCE would be well placed to serve as a secretariat and co-chair the Alliance, potentially jointly with the respective co-host of the GC3B conference.

Second, to **strengthen the sense of community among the existing and potential future endorsers and pledgers of the Accra Call, that will enable an inclusive process to capture their lessons and showcase their achievements, and also attract new supporters**, the GFCE would need to provide more stewardship in curating this connection. A more systematic approach to tracking and connecting the work already undertaken by the cyber capacity building community and key players in development and international cooperation that align with the Accra Call and the implementation of specific actions would benefit all and strengthen the GC3B's role as an action-oriented node in the international cyber cooperation ecosystem.

The consultations with the Accra Call supporters around their **Accra Call Action Stories,** that capture in a concrete way the progress and impact of the pledges made in GC3B 2023, offer an opportunity to inspire and mobilize the community towards the next GC3B.

GC3B Global Conference on Cyber Capacity Building

SUPPORT THE ACCRA CALL

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.

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

Read more about the Call and submit your support!

For more information, please email contact@gc3b.org.