GC 3B Global Conference on Cyber Capacity Building

GC3B Summary Report

Accra, Ghana | November 2023

GFCE Global Forum on Cyber Expertise

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP

CyberPeace Institute

WORLD ECONOMIC FORUM

MINISTRY OF COMMUNICATIONS & DIGITALISATION

CYBER SECURITY AUTHORITY CSA

FOREWORD

David van Duren, Director of the Global Forum on Cyber Expertise (GFCE)

For the first time in history, high-level leaders, experts on cyber security and capacity building, and the international development community across the world have gathered to work on common goals and solutions. The GC3B 2023 was a great gathering of minds, who came together to elevate discussions of cybersecurity into the global governance agenda.

This inaugural conference has been 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. The GC3B addressed the international need to increase **resources** for cyber capacity building, which is a key enabler for **sustainable development**, economic growth, and social progress. But most importantly: the **Accra Call for Cyber Resilient Development** was announced – a milestone document that provides a blueprint to mainstream cyber capacity building efforts with sustainable development plans through its actionable framework. The broad support of governments and organizations for the Accra Call demonstrates the global need as well as willingness to act now.

On behalf of the co-organizers, the Global Forum on Cyber Expertise, the Cyber Peace Institute, the World Bank, and the World Economic Forum, and on behalf of the host Ministry of Communications and Digitalisation and the Cyber Security Authority of Ghana, we thank all attendees, speakers and involved organizations, as well as the GC3B team behind the scenes, who contributed to cyber resilience for development through a shared belief in our mission to ensure a secure and free digital future.

We hope you had a most fruitful conference and that this report provides an insightful summary of the discussions that were held at the GC3B 2023.

TABLE OF CONTENTS

INTRODUCTION

The inaugural Global Conference on Cyber Capacity Building (GC3B) was held on 29-30 November 2023 under the common theme 'Cyber Resilience for Development'. The event was intended to raise awareness of the need for every nation to invest in their cyber expertise, and to encourage countries to work together to ensure a free, open, and secure digital world. The conference was co-organized by the Global Forum on Cyber Expertise (GFCE), the World Bank, the CyberPeace Institute, and the World Economic Forum, and hosted by the Ministry of Digitalisation and Communications of Ghana through the Cyber Security Authority (CSA).

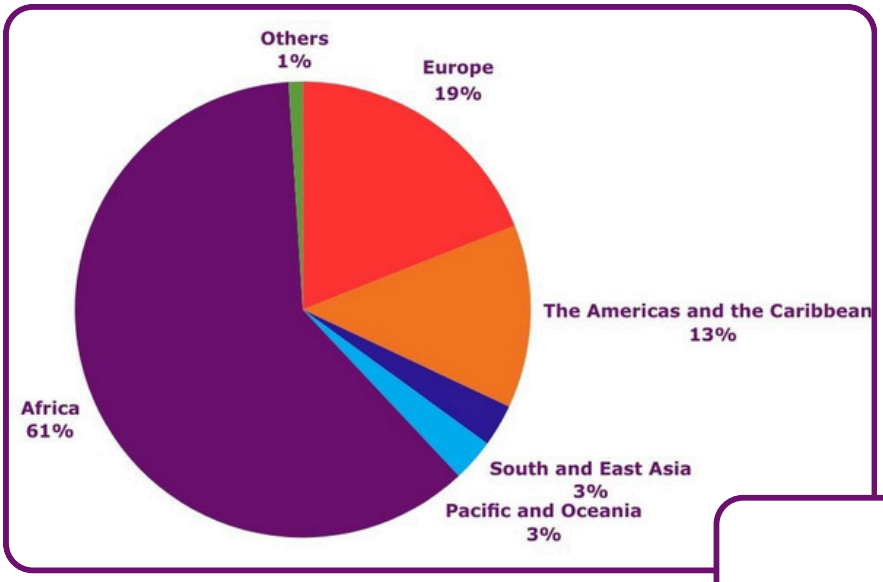
The GC3B offered a unique opportunity to the international, multi-stakeholder community to work on common solutions and address the international need to increase resources for Cyber Capacity Building (CCB), which is a key enabler for sustainable development, economic growth, and social progress.

In this first edition, the GC3B brought together leaders and experts from the global cyber and development communities. The attendance of high-level leaders and organizations from all sectors and regions ensured the event was multi-stakeholder and inclusive in its approach. Some key numbers on participant representation at the conference are visible below.

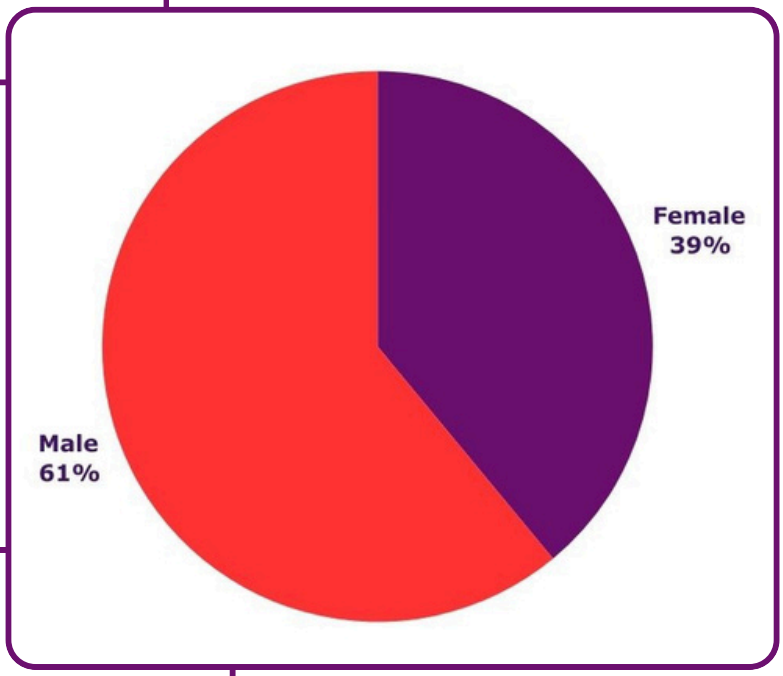
Going forward, the GC3B will take place every two years.

GC3B IN NUMBERS

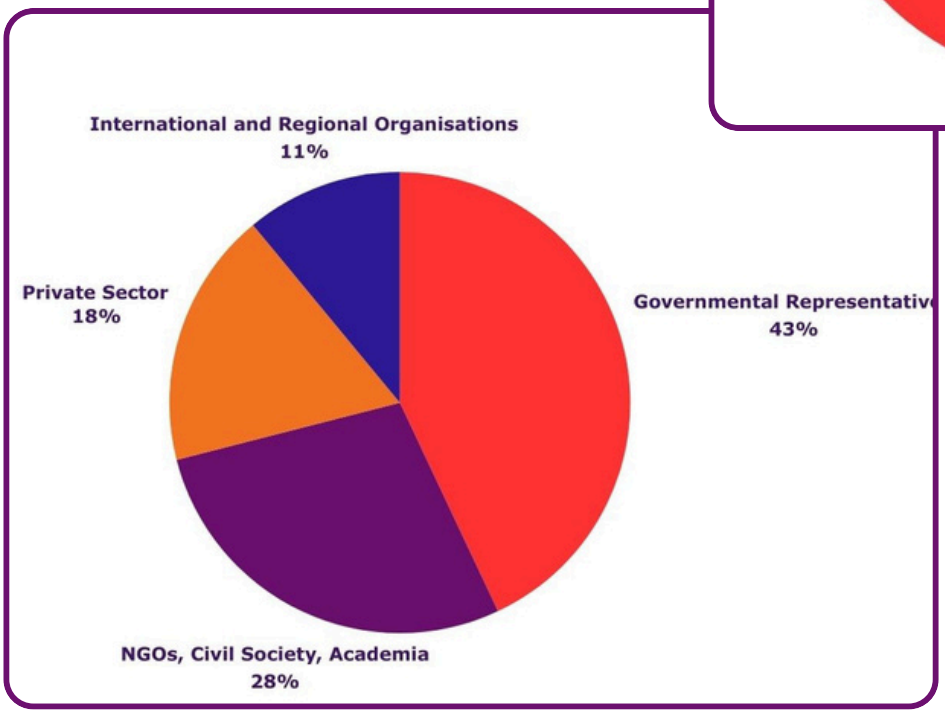
Regional representation



Gender Representation



Stakeholder Representation



KEY HIGHLIGHTS

Senior Presidential Advisor of Ghana H.E. Yaw Osafo-Maafo signs the Accra Call, in presence of Hon. Minister of Communications and Digitalisation Ursula Owusu-Ekuful (left) and Director-General of the Cyber Security Authority, Dr. Albert Antwi-Boasiako (right)

One of the GC3B highlights was the introduction of the Accra Call for Cyber Resilient Development, an outcome document that was endorsed by more than 60 governments and organizations. The Accra Call is an action framework articulating 16 non-binding, voluntary, direction-setting actions to mobilize all stakeholders towards strengthening the role of cyber resilience for sustainable development, advancing effective CCB, fostering stronger partnerships, and unlocking financial resources and implementation modalities

The Africa Agenda on Cyber Capacity Building (AA-CCB) was another noteworthy achievement presented at the GC3B. The document presents a shift from transactional to partner relationships, focusing on 'needs-driven' sustainable solutions. It is dedicated to pinpointing gaps in CCB and prioritizing strategic actions to bolster national CCB and fortify cyber resilience.

Chris Painter, President of the GFCE Foundation Board (center), Moctar Yedaly, Director of the GFCE Africa Hub (right), and Dr Martin Koyabe, Senior Project Manager African Union (left)

Chris Painter, President of the GFCE Foundation Board and Dr. Mactar Seck representative of UNECA, sign the MOU between the GFCE & UNECA

During the plenary session, UNECA and the GFCE signed a memorandum of understanding (MOU) to support cyber capacity development in African countries, addressing the significant need for cybersecurity professionals and institutional capacities.

In this common effort to ensure effective CCB globally, the conference sessions were divided into four pillars:

1

In '**Pillar 1: Making international development cyber resilient**', the integration of cyber resilience into sustainable development took center stage, emphasizing its role as an enabler of digital, economic, and social growth. Sessions under this pillar raised awareness of the added value of incorporating cyber resilience across the strategic priorities of developing countries.

2

In '**Pillar 2: Collaborating to secure the digital ecosystem**', public-private cooperation and multi-stakeholder cooperation emerged as key elements in addressing systemic challenges and vulnerabilities of the digital ecosystem. Two critical areas where such collaborations are needed were spotlighted: (1) *narrowing the cybersecurity workforce/skills gap*, and (2) *protecting critical infrastructure and essential services.*

3

'**Pillar 3: Cyber capacity building for stability and security**' dived into the role of CCB in strengthening the links between international security and sustainable development. Ongoing work at the UN was noted on issues including the framework for responsible State behavior in cyberspace and protecting the digital environment, including through the expansion of capacity building efforts.

4

'**Pillar 4: Operationalizing solutions**' zoomed in on good practices, tools, and practical solutions from CCB, particularly those that are of immediate assistance to protect development work from digital risks and threats. From closing the cybersecurity talent gap to strategically integrating cybersecurity into development programs, this pillar showcased demand-driven cybersecurity and capacity building solutions and practical initiatives.

In addition to the four thematic pillars, a dedicated conference track focused on the regional dimension of CCB, with five regional sessions for Africa, the Americas and the Caribbean, Southeast Asia, the Western Balkans, and the Pacific.

This GC3B was conceived as the first in a series of conferences to bring together high-level leaders and experts from around the world on cybersecurity capacity building and international development to work on common solutions in strengthening cyber resilience for development. During the event, it was announced that the next GC3B will be hosted by the Government of Switzerland, in Geneva in May 2025.

This summary report is a result of textual analysis of the recordings of GC3B sessions. It summarizes the main takeaways of the conference as a whole, rather than exploring the specifics of each individual session. The report was provided by DiploFoundation.

Patryk Pawlak, Head of the GC3B Program team

PILLAR 1: MAKING INTERNATIONAL DEVELOPMENT CYBER RESILIENT

The rapid expansion of digitalization and connectivity has brought numerous benefits to developing countries, while also exposing them to new risks and vulnerabilities. As digitalization increases, so does the need for robust cybersecurity measures to protect critical infrastructure. This complex issue requires the involvement of various international stakeholders, from governments and private sector entities to civil society and non-profits.

The World Bank, for instance, has committed to managing about $20 million in technical assistance programs, including cybersecurity maturity assessments and action plans to boost cyber capacity and resilience. Similarly, Mastercard invests heavily in cybersecurity, advocating for collective defense and building a cyber talent pipeline through public-private partnerships.

However, advocating for cybersecurity resources is challenging in a world with competing priorities. This is why it is crucial to integrate cybersecurity into all development sectors and to ensure that cybersecurity training and education align with the skills required across the workforce.

Developing countries need funding and market strategies for sustainable cyber resilience. The European Bank for Reconstruction and Development (EBRD) invests in private and public sector entities to achieve transitional goals aligned with the Sustainable Development Goals (SDGs), viewing cybersecurity as both an opportunity and a risk.

The private sector also plays a crucial role in this regard. Companies like Tech Experts provide managed security services, adapting to different regulatory requirements in various countries. However, the private sector faces challenges such as the scarcity of cybersecurity professionals and the need for continuous improvement.

The role of governments in promoting cybersecurity is also significant. Ghana, for example, is recognized as a leader in cybersecurity in West and Central Africa, having established a Cyber Security Authority, ratified international conventions, and passed a Cybersecurity Act.

However, assessing the overall impact of investments and capacity building projects on national economic and security outcomes remains a challenge. This is why there is a need for better evaluation and evidence-based approaches. This need applies just as much to national cybersecurity programs as it does to external funded cybersecurity projects. In both cases, there is a lack of a consistent framework for measuring improvement in cybersecurity outcomes. Monitoring and evaluation models (M&E), exemplified by the United Kingdom's approach, demonstrate intervention effectiveness for continued investment, and are used as the basis for evaluating both internal and external capacity building activities.

The international community must work together to fill these gaps and avoid geographical investment asymmetries in strengthening cyber resilience globally. This requires shifting from viewing CCB as a security policy tool to a development policy issue.

In conclusion, building a cyber-resilient international development landscape requires a multi-faceted approach. It involves advocating for cybersecurity resources, integrating cybersecurity into all development sectors, promoting cybersecurity training and education, and fostering international collaboration. It also requires the involvement of various stakeholders, including governments, private sector entities, civil society, and non-profits.

PILLAR 2: COLLABORATING TO SECURE THE DIGITAL ECOSYSTEM

Discussions at the conference revolved around the criticality of enhancing cybersecurity capacity building and resilience for critical infrastructure, which is essential for achieving sustainable development, economic growth, and social progress. The global challenge of closing the cybersecurity skills gap, especially in developing countries, was highlighted, emphasizing the need for international cooperation among governments, the private sector, and civil society. Gender imbalance in the cybersecurity workforce was also stressed, with stakeholders calling for the creation of opportunities for women and other underrepresented groups.

The GFCE emerged as a pivotal platform for effective capacity building cooperation. Supporting developing countries in cybersecurity requires a tailored understanding of their needs. Efforts to bridge the skills gap include donor support, training initiatives, and leveraging AI by companies like Microsoft. The International Telecommunications Union (ITU) concentrates on institutional and human capacity development, underscoring the formation of trustworthy teams and the importance of sharing resources while avoiding duplication of efforts. Meanwhile, the Organization of American States (OAS) promotes public-private partnerships, offering digital education programs, facilitating access to quality training, and designing national strategies to ensure sustainable CCB.

Speakers underscored the significance of CCB partnerships, acknowledging resource constraints and the need for diverse expertise. They emphasized the importance of involving all stakeholders, ensuring context-specific efforts, addressing potential challenges arising from political changes, and measuring long-term project impacts. CCB should be approached comprehensively, combining bottom-up and top-down strategies to align broad policy guidelines with varied CCB projects.

The cybersecurity community's need to anticipate and develop expertise in countering AI-related cyber threats through CCB was highlighted, considering cybercriminals' potential misuse of AI for fraud and automated attacks, which can lead to larger-scale incidents. Experts stressed that there is also a gap related to emerging technologies, which requires intentional education and workforce development to combat cyber threats. Focusing on fundamental cyber management and hygiene can effectively address various cybersecurity challenges. Initiatives like the InterCorp Network aim to prevent cyber offences through youth education on legal and positive behavioral aspects.

Cooperation within and between regions is essential both for CCB and for collective action to prepare for and respond to incidents. Regional organizations like the OAS were highlighted for their effective stakeholder convening, which is essential for sustainable development and cyber resilience. Learning from diverse regional experiences can enhance global cybersecurity solutions, acknowledging the value of both successful and unsuccessful cases.

The GFCE's establishment of regional hubs demonstrated effective cross-regional cooperation, as does the OAS collaboration with the European Union (EU), Organization for Security and Co-operation in Europe (OSCE), and other regional organizations.

Although institutions like regional organizations play a vital role, cooperation between and within countries is ultimately a matter of people working together. Activities that build personal relationships and prepare people for working together in their daily roles were strongly encouraged. This can be done through project activities such as events, training, exercising, or fellowship schemes.

The sessions concluded with a call for a holistic approach to cybersecurity, encompassing technology, policy, and human elements. Collaborative partnerships in global CCB were underscored, with examples like the United Kingdom government's integrated approach and ITU's Cyber for Good project. The importance of both bottom-up and top-down approaches in CCB, preparing for AI-related threats, and sharing knowledge and resources across regions were emphasized. Cross-regional cooperation in cybersecurity, through platforms like the GFCE, was encouraged for a safer cyberspace.

PILLAR 3: CYBER CAPACITY BUILDING FOR STABILITY AND SECURITY

Expert representatives from various countriesand organizations underscored the criticality of integrating cybersecurity into development and international security strategies. The speakers emphasized that cybersecurity should be a key pillar for development and security, particularly in developing states. These countries are actively seeking partnerships with more developed entities to assist in areas such as technical forensics, incident response, law enforcement, and public awareness of digital threats.

It was acknowledged that while digital transformation boosts economic growth, it also escalates cyber threats. Therefore, cyber resilience must be a mandatory element of digital development, obligating experts to develop and implement cybersecurity frameworks, policies, strategies, and legislation. The need for regional and international collaboration to bolster cybersecurity was also highlighted. This collaboration should include sharing incident experiences, capacity development, and aligning cybersecurity with sustainable development goals.

Speakers also emphasized the importance of educating citizens and policymakers to raise the national security baseline and foster a cybersecurity culture. They stressed the need for CCB development to enhance skills in the digital age and called for international cooperation and optimization of resources.

The need to complete cybercrime investigation and prosecution guidelines and share expertise with other countries was stressed. This could be achieved by enforcing the second additional protocol to the Budapest Convention, allowing for more efficient cross-border cooperation with necessary human rights and rule of law safeguards.

Experts underscored the importance of having a set of agreed-upon principles to implement CCB efforts effectively. Over the years, various initiatives have developed principles applicable in CCB, including the Busan principles (2011), the GFCE Delhi communique (2017), and the United Nations Open Ended Working Group (OEWG) consensus report (2021). Despite their different origins, these sets of principles are complementary and contain a recurring set of themes.

The session also discussed the challenges of applying a principles-based approach and how these should be overcome, including by building understanding of key terms, ensuring buy-in among different actors, and leveraging knowledge, tools, and resources from development actors to support implementation within the CCB field. On the challenges of defining key terms, for example, experts noted the value of translating technical cybersecurity language for diplomats and the importance of bridging the gap between technical experts and policymakers.

In recommending next steps, experts highlighted that the Internet Governance Forum (IGF) could play a crucial role in establishing global good practices and providing operational recommendations for CCB. Experts also stressed the need for practical guidance and tools to help stakeholders apply principles in various contexts, including integrating gender considerations and other values into CCB projects.

The 2022 ransomware attack on Costa Rica was discussed, emphasizing the necessity of robust legal frameworks and international law in the cyberspace. The speakers highlighted the strategies of Canada, the Philippines, and the African Union, stressing the importance of training officials in cyber law, geopolitical understanding, and national legal policy for preventing future cyberattacks.

PILLAR 4: OPERATIONALIZING SOLUTIONS

Closing the cybersecurity talent and workforce gap

The cybersecurity talent and workforce gap is a significant issue that needs to be addressed urgently. There is a shortage of nearly 4 million cybersecurity professionals globally, as well as a big gender disparity: Currently, only a quarter of the global cybersecurity workforce comprises women. This gap must be closed to foster diversity, innovation, and comprehensive strategies in cybersecurity.

Innovative approaches and unconventional strategies are necessary to make cybersecurity resonate with target audiences. For instance, pop culture and creative media can be used to influence career choices and inspire interest in cybersecurity. The perception of cybersecurity careers must also be redefined to attract and retain women. This can be achieved by emphasizing the diversity of roles and the accessibility of the field to non-technical backgrounds. Funding and support for programs that aim to bridge the gender gap are crucial for scaling and replicating successful models.

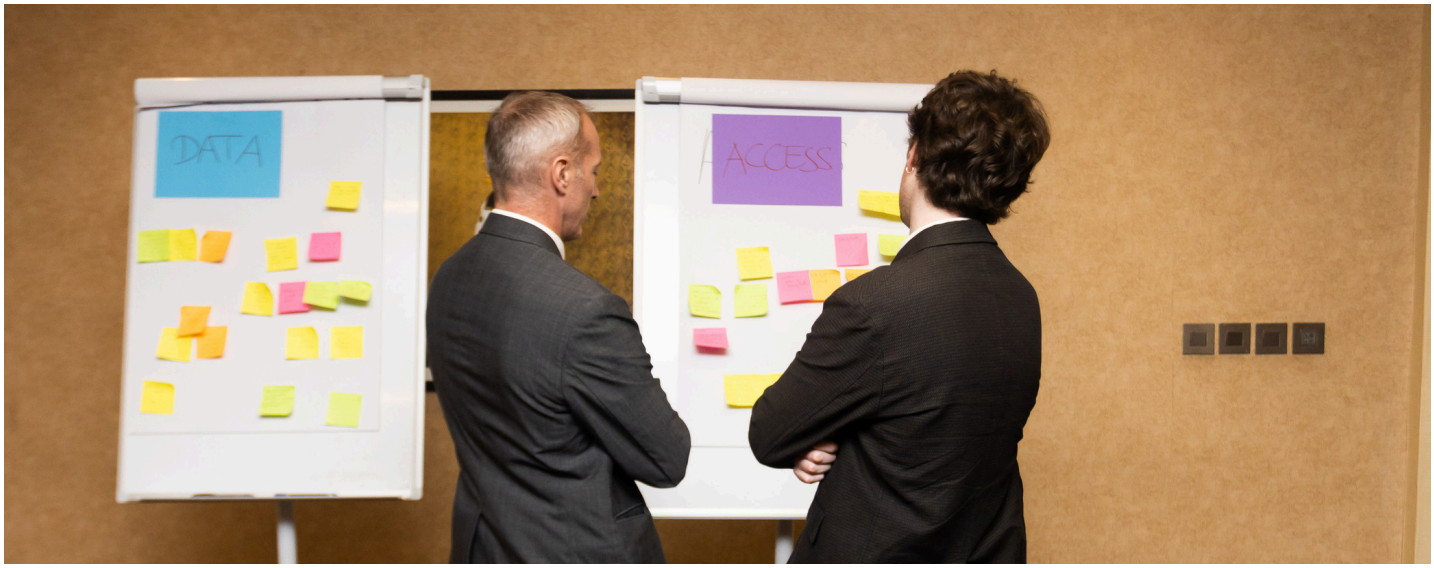
The discussion also highlighted the importance of starting cybersecurity education early, maintaining interest as girls grow older, and challenging societal norms that discourage women from entering the field. More hands-on practical activities, interactive learning sessions, and real-world connections are needed in cybersecurity education programs.

Public-private partnerships can also play a significant role in developing initiatives to attract and retain more women in the field. For instance, tax incentives for companies that employ women in cybersecurity roles could be established.

Another way to bridge the cybersecurity skills gap is skills-based volunteerism, where cybersecurity professionals volunteer their expertise to assist organizations in need. For example, some countries in Europe implement the cyber reserves concept where a network of volunteer experts supports government Computer Security Incident Response Teams (CSIRTs) in times of cybersecurity crisis. The need for increased awareness of available resources and the building of networks to connect organizations in need with potential support was underscored. In this regard, the World Economic Forum's Centre for Cybersecurity has launched a multi-stakeholder initiative - "Bridging the Cyber Skills Gap" - to raise decision-makers' awareness of the cybersecurity workforce deficit and advance the creation of a strategic cybersecurity talent framework featuring actionable approaches to help organizations create sustainable cybersecurity talent pipelines.

Several programs which are focused on assisting the cybersecurity needs of vulnerable communities, mentorship programs, and a community of cyber experts were discussed, including the United States Agency for International Development (USAID)'s Digital APEX Program, Standard Chartered's initiatives, and EU CyberNet. The sustainability of these models and the importance of long-term engagement, partnerships, and avoiding duplication of efforts were also emphasized.

CCB should involve all actors - government, civil society, academia, and the private sector - to drive change and ensure resilience. Collaboration between the private sector, NGOs, and governments on cyber hygiene and awareness is crucial, with the private sector developing platforms and NGOs conducting training. The Train the Trainer (TOT) method was discussed as an effective approach to CCB, with the importance of tailoring training to local contexts and legal systems emphasized.



The sessions also highlighted the importance of community in building technical capabilities, fostering networks of trust and information sharing, and promoting professional development. Long-term capacity building and training of trainers were identified as essential components in sustaining technical cyber capacity. For instance, a community in the Philippines was established for weekend training sessions to accommodate government employees, evolving to include programs for women and career changers in cybersecurity. However, challenges related to sustainable funding for community initiatives were underscored, necessitating the alignment of donor programs with local needs. The importance of co-designing programs with donors to ensure they meet the community's needs and have a measurable impact was emphasized. Director-General of the Cyber Security Authority, Dr. Albert Antwi-Boasiako (right)

Cybersecurity needs are specific to regions, and capacity building programs must be tailored to these needs. Good practices from around the world should be considered and needs assessments are crucial. The role of regional centers in strengthening local, regional, and international ownership of cybersecurity actions was discussed. Regional CCB centers were positioned as central hubs for knowledge sharing, collaboration, and empowerment, requiring sustainability, regional ownership, and transparent decision-making processes. The challenges of securing funding and political commitment for these centers were also highlighted. There was a call to adapt regional centers to local contexts, considering geopolitical aspects, political will, and financial support. But addressing diversity within regions is challenging. A sub-regional approach and building communities within smaller formats can be more effective.

Securing funding and political commitment were deemed crucial to transition from external funding to regional and national ownership and contributions. For instance, externally facilitated activities designed by donors and their implementors may lack ownership and therefore have weak sustainability. Conversely, locally driven, self-designed capacity building initiatives can offer a more promising avenue for ownership and long-term change. To overcome shortcomings in the implementation of CCB actions, all involved stakeholders should seek to embrace established good practices, for example the tailoring and integration of training courses into the curricula of national academies (police, judges, etc). Examples of such successful capacity building practices in the fight against cybercrime were shared, including the freezing of significant crypto currency assets in Sri Lanka and training of law enforcement, judges, and prosecutors in Benin.

The dedication and motivation of individuals involved in CCB, who seize opportunities and drive change, are recognized as key factors in the success of these initiatives.

Mainstreaming cyber resilience

The cyber resilience of the energy grid, communications infrastructure, and financial services were discussed.

The energy sector is identified as a high-risk critical infrastructure sector, witnessing a 24% increase in cyber-attacks in 2022. It confronts dynamic challenges due to increased digitalization. With more actors entering the grid, its vulnerability has increased, necessitating updated security measures. Millions of consumers contributing personal data to distribution companies pose risks of potential data leaks. The sector experiences intensified cyber-attacks due to digitalization and standard protocols, exacerbated by the increased attack surface introduced by Distributed Energy Resources (DERs). The sector's architecture, not initially designed with security in mind, requires new policies and standards, and crucial sector-wide risk management and information sharing. Integrating Internet of Things (IoT) devices on the grid also adds to the attack surface, demanding protective measures.

Learning from the energy sector's experience with Operational Technology (OT) and Information Technology (IT) benefits other sectors such as transportation and water utilities. Asset inventories and vulnerability mapping are deemed crucial, emphasizing the need to integrate cybersecurity into infrastructure investments from the project's outset rather than treating it as an afterthought.

Digital financial services have become essential for strengthening financial inclusion worldwide. Cyber resilience should be a prerequisite for developing a safe and responsible financial inclusion ecosystem and securing the rapid development of financial services. The case of Africa, in particular, was discussed during a dedicated session. Barriers to improving the cyber resilience of Africa’s digital financial services were enumerated, including consumer protection issues, lack of trust in digital channels due to fraud and inadequate customer recourse, inadequate regulatory frameworks and enforcement, education and awareness gaps among consumers regarding cybersecurity risks, identity theft, and cultural challenges related to trust. Some challenges local banks face include a lack of information sharing after cyber-attacks, financial constraints, and the need for skilled cybersecurity personnel. It was noted that a multi-faceted approach to improving cybersecurity resilience in Africa's digital financial services is needed, involving cooperation, education, regulatory frameworks, and leveraging global best practices.

The security and resilience of communications infrastructure are critical for the stability and safety of global communications and, by extension, for strengthening economic growth and ensuring the general wellbeing of people around the world. As cloud services gain significance, concerns arise about nation-state actors targeting them. Collaboration is crucial to understanding and defending against evolving threats. Cloud services are designed with resiliency in mind, incorporating redundancy and safeguards. This involves a shared responsibility between providers and customers to ensure adaptability based on business requirements.

The EU has directives for the resilience of subsea cables, including strategies, risk assessments, incident response teams, and designating cables as critical infrastructure. However, inherent complexities in proactively addressing cybersecurity concerns in Africa, a region contending with challenges stemming from capacity and capability limitations, were acknowledged. Notably, attention was directed towards the 'African Agenda on Cyber Capacity Building,' an initiative spearheaded by the African Union Development Agency. This initiative, poised to enhance capabilities and navigate technology-related challenges, signaled a commitment to fortifying the region's cybersecurity posture.

Strategic interagency cooperation and creation of national teams were proposed to drive transformative change in combating cybercrime. Political will at the state leadership level is crucial for developing a solid legal and institutional framework to combat cybercrime. Acknowledging the vital role of the private sector, a call was issued for private entities to contribute to awareness, deliver comprehensive training, and bridge gaps in understanding technological concepts. The necessity of cross-section learning and cooperation has already been highlighted by the World Economic Forum, which through its Centre for Cybersecurity is enhancing cyber resilience globally across industries through the Cyber Resilience in Industries initiative. This public-private platform gathers decision-makers to raise awareness of cybersecurity as a strategic priority, generate insights, and develop and scale forward-looking solutions to mobilize action for ensuring secure industry transformation.

The discussion turned to outer space, where existing legal frameworks such as the Outer Space Treaty and the Registration Convention were deemed robust. These could be strengthened rather than new regulations created. Policymakers should adopt international, risk-based, consensus-driven cybersecurity standards, such as those from ISO/IEC and NIST, to harmonize efforts.

The imperative for international cooperation and the involvement of the highest government authorities in effective cyber crisis management took center stage. Clear legal bases, national cyber crisis management plans, and preparedness measures were underscored as foundational elements. Crisis management governance structures must ensure strategic, operational, and technical cooperation. Operational and strategic challenges in responding to cyber crises were delineated, emphasizing the essential elements of clear communication, legal frameworks, decisive leadership, sector integration, trust, and compliance. Governance structures for crisis management, cooperation across strategic, operational, and technical levels, and the necessity for local capacity building and training were identified as necessary to enhance cyber resilience. Public awareness and education were deemed prerequisites for establishing a baseline for cyber hygiene. International and regional cooperation is crucial for managing cross-border cyber incidents, with existing frameworks and platforms facilitating collaboration. However, varied definitions of cyber crises among countries, contingent upon risk appetite and specific criteria, were acknowledged.

Critical elements for scaling cybersecurity tools and solutions effectively were examined, emphasizing stakeholder engagement, partnerships, socio-economic and cultural understanding, impact measurement, and feedback loops. The discussion focused on comprehending cultural contexts, engaging local communities, and constructing sustainable, scalable cybersecurity solutions. The importance of tailoring cybersecurity solutions to cultural differences and social norms was highlighted, emphasizing creating trust and ensuring solutions are embraced within diverse communities. Education and awareness campaigns are crucial in overcoming the digital divide and should be targeted and localized to the audience's needs. Cybersecurity education should be accessible and localized, suggesting that materials be translated into local languages and distributed through existing community channels. The role of women in cybersecurity, scalability challenges, and the significance of education and awareness campaigns were underscored, with specific mention of the Global Cyber Alliance Cybersecurity Toolkit as a resource catering to various stakeholders.

Best practices for enhancing cyber resilience in low-income countries through public-private partnerships were brought up. Partnerships are needed to address challenges within the cyber environment, where individual efforts are insufficient. They should be result-oriented, and a well-functioning institutional arrangement involving multiple agencies with cybersecurity mandates should be in place. Proactive leadership is also necessary to drive cybersecurity initiatives.

Director-General of the Cyber Security Authority of Ghana, Dr. Albert Antwi-Boasiako, with World Bank representatives Anat Lewin and Oleg Petrov, presenting Ghana as a case study in strengthening their cyber resilience

A successful example of enhancing cyber resilience in low-income countries through public- private partnerships is the Togolese model for establishing a computer emergency response team (CERT) under a public-private partnership with a security operations corporation (SOC). Togo established a regulatory framework to create a sustainable cybersecurity ecosystem involving both public and private sectors. The country passed a cybersecurity and cybercrime law in 2018, followed by decrees to create the National Cybersecurity Agency (ANSI) and Cyber Defense Africa (CDA). Togo identified essential services operators (critical infrastructure) and established a detailed contract of delegation of services between ANSI and CDA. CDA is a joint venture between the Republic of Togo and the Asseco Group, a Polish software group. CDA operates the Togo CERT and a SOC, providing cybersecurity services within and beyond Togo. ANSI regularly controls CDA's delivery of services through service-level agreements (SLAs) and can sanction CDA for non-compliance.

A document outlining Ghana's five-year journey in cybersecurity development, which could serve as a valuable lesson for other nations, was launched during the session on 'Integrating cybersecurity in development assistance programs'.

The discussions underscored the importance of trust, timely threat intelligence sharing, and the role of laws and regulations in promoting information sharing for effective cybersecurity.

Trust was repeatedly emphasized as a critical factor for effective information sharing. Without trust, stakeholders may hesitate to share sensitive information, impeding cybersecurity efforts. Sharing threat intelligence must be timely, as delayed sharing can make information less useful because cyber threats can evolve rapidly. Laws and regulations can support and promote information sharing by providing a framework that ensures confidentiality and encourages participation from various stakeholders. Tools and standards, such as TLP and MISP, were recommended for secure and standardized information sharing.

Different sectors may have specific needs and considerations regarding information sharing. It is important to understand these nuances to facilitate effective cross-sector collaboration.

Despite recognizing the importance of information sharing, challenges faced by CERTs, such as staffing and resource limitations, were acknowledged, necessitating the development of a skilled cybersecurity workforce.

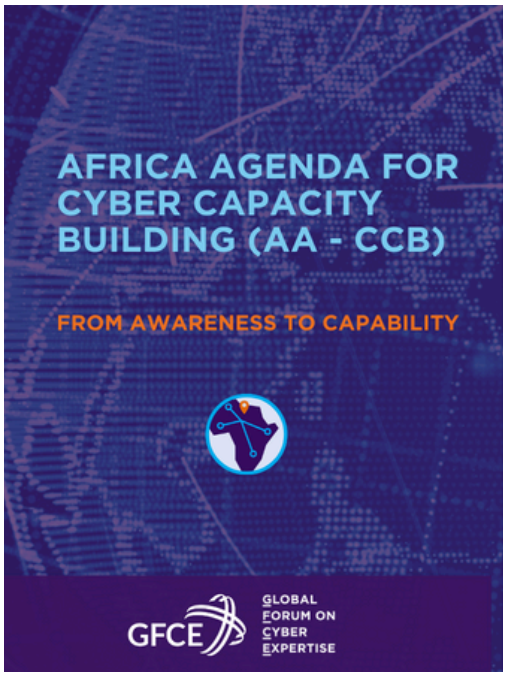
REGIONAL SESSIONS

Cyber needs of countries and regions are nuanced, context-dependent, and unique in a way that is often difficult to capture by the traditional supply-driven model of capacity building. Therefore, the GFCE's long-term objective is to ensure that the supply-driven tradition is converted into a demand-driven model by capturing the needs, expertise, and evolving capacities of countries.

The GFCE's regional presence is a key factor in bridging national and regional needs and contexts to global capacities, funding, and processes. Working on the regional level enables the GFCE to naturally take on a coordination or alignment role to ensure a demand- driven approach, prioritizing countries' and regions' needs.

The GC3B covered five regions.

Africa



The session summarized a project supported by the Gates Foundation that led to the development of the Africa Cyber Expert (ACE) community and the establishment of the Africa CCB Coordination Committee, which serves as a matchmaking and clearing house for CCB cases in the African continent. Building upon the outcomes of this project, the GFCE announced the GFCE Africa Hub at GC3B2023. The main objective of the GFCE Africa Hub is to address the critical need for strengthening CCB and cyber resilience in Africa.

The Africa Agenda on CCB was presented. It displays a shift from transactional to partner relationships, focusing on 'needs-driven' sustainable solutions. It is a collaborative effort between the AU and the GFCE.

The Agenda outlines six priority areas for CCB. It calls on actors, stakeholders, and states to invest, advocate, and implement actions nationally and regionally. Tasks include exchanging awareness norms and regional frameworks (like the Malabo convention), promoting South- South knowledge exchange, youth and education investment, and international partnerships.

Americas and the Caribbean

Tereza Horejsova, GFCE Outreach Manager, and Veronica Ferrari, Association for Progressive Communications

The session analyzed how National Cybersecurity Strategies in the region have incorporated gender perspectives. It included practical illustrations of how selected countries have advanced in this field, along with an examination of the challenges and prospects in the region, discussing the importance of incorporating a gender perspective in cybersecurity policies. The OAS, the home of the GFCE Hub for the Americas and the Caribbean, is engaged in efforts to support the inclusion of a gender perspective in cybersecurity policies throughout the region.

International civil society organizations like APC already see cybersecurity as a human rights issue. There are varying exposures to vulnerabilities. A gender approach to cyber means understanding differentiated risks and needs and having awareness on how to ensure that gender mainstreamed policies benefit everyone. Speakers stressed there needs to be a multi-stakeholder approach to policies, such as mapping existing voices, engaging those actors, and having accountability.

The GFCE presented its initiatives to ensure gender equality in cyberspace and CCB, as outlined in the document on Mainstreaming Gender in CCB (GFCE AM 2022). This includes several programs to support this commitment; such as Women in CCB (WiCCB) Network, which focuses on connecting women professionals, raising awareness, and promoting inclusion and knowledge sharing, or the Women in International Security & Cyberspace Fellowship (WiC).

South-East Asia

The session pointed out some of the main gaps in CCB in the region and how to address it through multi-stakeholder cooperation. It was pointed out that ASEAN leadership support is the key to successful cyber programs in the region.

Allan Cabanlong, GFCE Regional Director for South-East Asia

The ASEAN Leaders Statement of Support on Cybersecurity Cooperation and Capacity Building underscores a pivotal commitment to fortifying the region's cybersecurity resilience. This serves as a steadfast call to action for sustained efforts in bolstering cybersecurity across ASEAN nations. While there is room for greater stakeholder involvement, ASEAN's focus on understanding local contexts and building on successful initiatives is a promising strategy for the future.

ASEAN, in partnership with other countries, has organized various cybersecurity working groups and cybersecurity centers of excellence across the region. The ASEAN Singapore Cyber Security Center of Excellence (ASCCE),facilitated by the Cyber Security Agency (CSA) of Singapore, provides capacity building programs for the ASEAN member states as well as other regions that need capacity; the ASEAN-Japan Cybersecurity Capacity Building Center also provides physical and online training for the ASEAN member states with the endorsement of ADGMIN and ADGSOM. This demonstrates that Southeast Asia recognizes cybersecurity as an enabler in the development of the digital economy.

ASEAN's approach to cooperation is characterized by consultations at senior levels and working-level relations at the operational level.

Pacific

The GFCE Pacific Hub was officially launched at the Pacific CCB Coordination Conference (P4C) in Fiji, in October 2023. The session also focused on CCB priorities typical for this region. The primary difficulty identified in the Pacific region is the implementation of strategies due to a lack of capacities and capabilities.

The importance of scaling up domestic capabilities within countries to enable better engagement and cooperation at the regional level was noted. The potential of regional cooperation through information sharing and incident management capabilities to bolster the Pacific's ability to respond to cyber threats was emphasized. The goal is to build collective resilience through a unified Pacific voice on the international stage and to build trust and capabilities within the region. There is a willingness to cooperate, and a political and collective enduring partnership is seen as necessary. However, the sustainability of programs and limited absorption capabilities will require a re-evaluation of how they are delivered.

Looking ahead, the Lagatoi Declaration on Digital Transformation of the Pacific solidifies efforts for regional cooperation and leverages a unified Pacific voice in international conferences and meetings.

Strategic partnerships and initiatives in both the private and public sectors are seen as key to integrating regional actors for a whole-of-government effort. Examples of this include the roadshow in Samoa with CERT NZ, SamCERT, and other partners, and the P4C co-organized by the GFCE Pacific Hub and the Oceania Cyber Security Centre (OCSC), on behalf of the Partners in the Blue Pacific, which represented a landmark effort for future cooperation in the region.

The need to avoid duplication and repetition of similar, outdated training programs, and instead focus on needs-based support was highlighted. This includes not only training and awareness raising, but also enabling access to the latest and most secure technologies for the region, supporting high-quality tech for government, and patching vulnerabilities wherever possible.

Western Balkans

The session highlighted several key issues and areas of cooperation in the realm of cybersecurity. The importance of cybersecurity in maintaining trust in government, particularly in the face of increasing cyber-attacks, was underscored. This makes the development of robust cybersecurity capabilities essential for the protection of societies and the preservation of digital sovereignty in Western Balkan nations.

Hon. Slavica Grkovska, Deputy Prime Minister of North Macedonia

The challenges mentioned in the session include a lack of a multi-stakeholder approach, insufficient technical standards, and a lack of institutionalized cooperation in the region. Speakers emphasized the need for a more unified response to cybercrime and better coordination among donors, implementers, and beneficiaries. There was also a call for greater trust in the workforce's ability to manage cybersecurity across society.

Beyond technical solutions, the session highlighted the need for human resources to manage cybersecurity. The prevalent cybersecurity workforce gaps must be addressed through education, professional training, and hands-on experience. The role of academia in this regard was emphasized.

The session also identified several actors of cooperation, including the Western Balkan Centre of Excellence (WB3C), which aims to create more comprehensive resilience and commitment at the government level. Other examples of cooperation include the Berlin Process with German Corporation for International Cooperation (GIZ), the Geneva Centre for Security Sector Governance (DCAF) projects, and OSCE study trips in the region combining policy and technology.

ACKNOWLEDGEMENTS

The GC3B co-organizers are filled with a profound sense of gratitude and optimism, and thank the Steering Committee members and our sponsors for their invaluable support in shaping the conference's objectives and program. Their commitment and dedication have made the GC3B 2023 a truly impactful and memorable experience that has been crucial in shaping the future of cybersecurity.

Steering Committee

Government of The Netherlands

Government of France

Government of the United States

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

Government of Switzerland

Government of Australia

Government of Canada

Government of New Zealand

UK Government

Government of the United Kingdom

European Union

Government of Singapore

Government of Germany

Government of the Cook Islands

Sponsors

Microsoft

REGERINGSKANSLIET
Ministry for Foreign Affairs
Sweden

BAE SYSTEMS

Africa Connect 3

WACREN

LOOKING AHEAD

The second iteration of the Global Conference on Cyber Capacity Building will take place in **May 2025 in Geneva**, hosted by the Government of **Switzerland**. We look forward to welcoming you there for another memorable convening that will enable a prosperous digital future for all.

Stay tuned for more information!

Contact

For more information, please reach out to **contact@gc3b.org**.

Stay updated with our news on our website at: **gc3b.org**, follow the **#GC3B23** and follow us on social media:

@thegc3b

Global Conference on Cyber Capacity Building