GFCE GLOBAL FORUM ON CYBER EXPERTISE

28 NOVEMBER | ACCRA, GHANA

GFCE Annual Meeting 2023 Report

PREPARED BY THE

GFCE SECRETARIAT

DECEMBER 2023

TABLE OF CONTENTS

Executive Summary

This report provides a comprehensive overview of the key highlights, discussions, and outcomes from the highly successful Annual Meeting 2023. The meeting brought together cybersecurity experts, policymakers, industry leaders, and other stakeholders to explore and address the evolving challenges and opportunities in the field of cybersecurity.

Throughout the event, diverse sessions and insightful discussions delved into the progress made and persistent challenges in the ever-evolving cybersecurity landscape. The strength of the GFCE Community was prominently displayed, showcasing a collective commitment to fostering cyber capacity building globally. The rich interactions and collaborative spirit witnessed during the meeting exemplify a shared vision for creating a safer, more resilient cyber environment.

Reflecting on the highlights, a resounding theme emerged — a robust commitment to the cause of cybersecurity. The sessions not only facilitated the exchange of knowledge but also resulted in tangible action points and identified areas for sustained collaboration. Recognising the dynamic nature of cybersecurity challenges, the GFCE acknowledges the need for persistent efforts and innovative approaches.

As we transition into 2024, the GFCE reaffirms its steadfast commitment to leading global initiatives to enhance cyber capacity building. With a collaborative spirit, the organisation is dedicated to contributing to a more secure and resilient digital future for all. Embracing the evolving landscape of cybersecurity with vigilance and adaptability, the GFCE remains at the forefront of global efforts to address the challenges of our digital age.

PROGRAM OVERVIEW

Global Forum on Cyber Expertise (GFCE) Annual Meeting 2023

From Local Context to Global Action
Coordinating Paths to Cyber Resilience

28 November 2023

Time (local time):	Room 1	Room 2	Room 3
08:00 – 10:00	Women in Cyber Capacity Building (WiCCB) Breakfast: Sharing Regional Perspectives		
10:00 – 11:00	Community Showcase	GC3B Research Workshop	Internet Infrastructure Initiative (Triple-I) Workshop
11:00 – 12:00			
12:00 – 13:00	Lunch (Networking event)		
13:00 – 14:00	Official Opening – GFCE Annual Meeting 2023		
14:10 – 15:40	Working Group C Session: Addressing Cybercrime Enabled by Emerging Tech	Working Group D Session: Building a Cyber Resilient Culture	Internet Infrastructure Initiative (Triple-I) Workshop
15:40 – 16:10	Break		
16:10 – 17:40	Working Group A Session: Evolving National Cybersecurity Strategies	Working Group B Session: Ensuring Resilient Critical Information Infrastructure	Internet Infrastructure Initiative (Triple-I) Workshop
17:40 – 21:00	GC3B Informal Cocktail Reception (Networking event)		

Women in Cyber Capacity Building (WiCCB) Breakfast: Sharing Regional Perspectives

The WiCCB Network plays an important role in helping, coordinating, and complementing stakeholder efforts to mainstream gender in CCB through the GFCE's platform. It provides a space for stakeholders to share information on projects and initiatives, trends and developments based on common understanding and values.

Background of the session:

The Women in Cyber Capacity Building (WiCCB) Breakfast: Sharing Regional Perspectives served as an informal gathering of all gender equality promoters. It sought to connect all relevant actors across cyber and development to ensure long-term and sustainable cooperation for gender equality in the field.

This event was designed to allow women and equality supporters to connect and/or create stronger ties. Within this informal setting, we were delighted to see the participants enthusiastically seize this opportunity to share and connect with one another.
The session was built around several activities, namely three speaker sessions, informal networking moments, and a white board activity.

Key activities:

The session featured speakers advocating for gender equality, delving into the issue of gender inequality within the CCB. Key points included the limited representation and opportunities for women. The exploration of root causes highlighted the distinction between equal opportunity and equality-focused policies. Proposed solutions involved awareness-raising initiatives, region-specific knowledge sharing, and enhanced communication among female professionals. There were calls for structural changes, particularly advocating for the inclusion of women in high-level roles. Various solutions were suggested, ranging from theoretical reflections to infrastructure reforms, with a specific focus on SDGs, improving education quality, and fostering international partnerships.

The White Board activity involved strategically placing boards around the room with three open questions addressing the WiCCB Network members. These questions sought insights into preferred activities and events, topics of interest, and any additional ideas for consideration. The responses collected during this activity will contribute to shaping the WiCCB 2024 agenda.

Key takeaways:

Both speakers and participants focused on a solution-based approach in the session, and attendees agreed that real-time change in CCB will be made through the implementation of certain elements and concepts. First, it was noted that it must be recognized that men and women have different tools available to them, and that this is often a result of systematic biases. To address this, there must be equal opportunities and venues for women in CCB. Such opportunities should be based on a clear understanding of the inequalities within CCB. Most important is the creation of educational opportunities, with a special focus on educating young girls. It was also highlighted that such action should not only focus on women's empowerment but should also include awareness-raising mechanisms. Finally, this awareness of systemic biases should be built into policies, and that policy should be designed to reflect a mindset of gender equality in CCB.

Community Showcase

Background of the session:

The Community Showcase provided a strong foundation for understanding the work of the GFCE Members and Partners, and aimed to enable better collaboration, information exchange and knowledge sharing amongst the GFCE Community. With a total of seven showcases, this session presented the GFCE Community with an opportunity to share good practices, recent deliverables or new initiatives.

Key activities:

Each speaker had the opportunity to discuss a project they wished to introduce or highlight to the GFCE Community. Projects discussed included manuals of cybernorms, initiatives to increase multi-stakeholder engagement in CCB processes, and innovative bottom-up approaches to CCB, demonstrating the rich diversity in community efforts. Other initiatives showcased the importance of knowledge sharing and the effective implementation of such knowledge, demonstrating the efficiency of cooperation between academia and policy analysts. Overall, these presentations commonly highlighted the range of solutions that governments, private companies, academia, NGOs and CSOs are innovating to address the remaining gaps and insecurities related to digitalization.

Key takeaways:

The opportunity to present their work and discuss in an open format with GFCE Community members was warmly welcomed by participants. Moreover, they all agreed on the importance of such sessions going forward, as a means to foster a high level of expertise, synchronisation of policies and initiatives, and a common approach to cyber capacity building.

GC3B Research Workshop

Background of the workshop:

The GFCE Research Committee organised a workshop around the GC3B thematic areas, aiming to foster scholarly research on cyber capacity building from an interdisciplinary perspective and enhance dialogue between the research community and policymakers. Following an open call, eight papers were selected to be presented and discussed by their main authors.

Throughout the process, the Research Committee was supported in their review process by members of the GC3B Program Team, along with academics from the University of Ghana (UG), who provided an important link to local knowledge institutions. Additionally, a dozen students from UG were invited to participate in the GFCE Annual Meeting, as well as the GC3B activities.

Key activities:

The session, skillfully moderated by the chair, featured three distinct panels, each led by a dedicated Chair and Discussant.

Panel 1 delved into the symmetries in the development of national cybersecurity policies in Latin America, the challenges to cybersecurity strategy in SADC, and perspectives on cybersecurity capacity building measures in the South Caucasus.

Panel 2 explored the impact of capacity development activities on the effective prevention of cyber violence against women and girls, cybersecurity in the era of quantum advantage, and a review of the international cooperation regime for the control of cybercrime in Nigeria, offering valuable lessons and recommendations.

Panel 3 focused on developing a cybersecurity and technology roadmap for humanitarian non-governmental organisations and conducted a critical discourse analysis of cybersecurity in Malawi media.

The selected papers collectively provided comprehensive insights into diverse and crucial topics within the realm of cybersecurity.

Key takeaways:

The workshop highlighted the importance of involving academic voices in cyber capacity building discussions and debates. Moreover, it showed examples of how interdisciplinary research from various regions around the world can add value to ongoing conversations in the field. Moving forward, the papers presented will undergo a final editing phase based on the feedback provided during the workshop discussions. Finally, it is expected that the papers will be published in a journal as a special issue.

Internet Infrastructure Initiative (Triple-I) Workshop

The GFCE Triple-I intends to facilitate awareness raising and capacity building events in different regions of the world to enhance justified trust in the use of internet and/or email in those regions. The GFCE Triple-I seeks to build upon and complement existing know-how, while raising awareness on a number of state-of-the-art open internet security standards and instigating uptake of those by building on good practice experiences.

Background of the workshop:

The workshop supported participants who wanted to learn more about open internet standards such as DNSSEC, DANE, RPKI, ROA, TLS, DMARC, DKIM, KINDS, MANRS, SPF, and IPv6. The workshop helped support more trusted communications, promoting inspiration from good practice experiences from the African region and elsewhere that helped improve reliability of the internet and collaborative security. It also encouraged participants to work together to develop and commit to specific actions that will help improve the region's internet economy.

Key activities:

The workshop took place across the whole day, divided into three blocks:

Block I: Better Use of Today's Open Internet Standards, moderated discussion about the use and usefulness of Open Internet Standards such as DNSSEC, TLS, DANE, RPKI, ROA, DMARC, DKIM, SPF and IPv6.

Block II: Inspiration from Good Practice Actions, delved into successful practices in the cybersecurity landscape, covering topics like the Internet Resilience Index, offering insights into a country's internet resilience across infrastructure, performance, security, and market readiness; MANRS, focusing on its rationale, development, and deployment; KINDNS, exploring its rationale, development, and deployment; the Coalition for Digital Africa, outlining its aims, activities, and future plans; and the Global Cyber Alliance, providing cybersecurity toolkits tailored for end users.

Block III: Planning for a More Trusted Internet: Marketplace for Action, facilitated brainstorming, based on the input discussed over the day, and introduction of a possible way forward leveraging the "justified trust in the use of the Internet and email" throughout Africa.

Key takeaways:

While the final report of the workshop is being finalised, workshop coordinators will continue working on a follow-up action plan based on the discussion. The idea is for the workshop to crystalise a more sustained effort to strengthen the resilience of the internet across Africa. The report, presentations, pictures and other materials will be available in due course via the GFCE Triple-I page on the GFCE website.

Opening Remarks

The GFCE Annual Meeting 2023 opened with welcome remarks from the GFCE leaders, Directors of GFCE Secretariat, President of the GFCE Foundation Board, Co-Chair of the GFCE Advisory Board, Co-chair on behalf of the Netherlands and Co-chair on behalf of India.

Directors of the GFCE Secretariat welcomed participants to the 2023 Annual Meeting, reflecting on the organisation's eight-year journey of fostering community collaboration and knowledge sharing. They highlighted the Annual Meeting's goal to mobilise Members, Partners, and the broader cyber capacity building community for enhanced international cooperation, introducing the inaugural Global Conference on Cyber Capacity Building (GC3B) and acknowledging the stability and leadership provided by GFCE Members and Partners. Additionally, the establishment of the GFCE Foundation in 2019 to support cyber capacity building endeavors was mentioned, showcasing the GFCE's growth and a commitment to future strengthening. They also expressed gratitude for attendees' participation, emphasizing the GFCE's maturation in cyber capacity building since 2015 and its unique member-driven, neutral platform. They outlined Secretariat support through working groups, regional teams, and hubs, highlighting a shift towards implementation and a demand-driven approach. The upcoming GC3B was discussed, concluding with thanks for the continuous support of the GFCE Community.

Co-chair on behalf of the Netherlands commended the GFCE community for their active engagement in capacity building efforts and emphasized the Forum's significance in fostering a multi-stakeholder, regional approach to cybersecurity. She highlighted the Netherlands' commitment to the GFCE's vision, especially in promoting gender equality, supporting UN initiatives, and addressing the challenges of cyber resilience in development. She called on like-minded donors to sustain the momentum generated through the Accra Call and invited the community to share ideas for the Foundation's future endeavors.

Co-chair on behalf of India expressed heartfelt congratulations to the GFCE Secretariat for convening the annual meeting. Acknowledging the importance of international collaboration on cyber security and resilience, he commended the efforts of Co-chair on behalf of the Netherlands and emphasized the evolving role of GFCE in global cyber capacity building. Highlighting India's contributions, he outlined various initiatives, including the Cyber Surakshit Bharat program and the Digital Personal Data Protection Act 2023, showcasing India's commitment to creating a secure cyberspace. He concluded by urging members to coordinate efforts for cyber resilience and fostering collaboration among nations for a safer digital future.

GFCE President of the Foundation Board underscored the remarkable growth of the GFCE, expanding from 42 members in 2015 to over 200 in 2023. He emphasized the vital role of sustained engagement with cyber capacity and development communities. In his address, he proposed the creation of a Strategic Steering Committee to guide future directions and advocated for the expansion of the Foundation Board. Finally, he expressed gratitude to attendees, highlighting the significance of collaboration and knowledge exchange in shaping the global landscape of cyber capacity building.

Co-chair of the GFCE Advisory Board expressed her heartfelt appreciation for the successful culmination of the GFCE Annual Meeting 2023. She emphasized the significant contributions of the GFCE Advisory Board (AB) since its establishment in 2016, underscoring its vital role in providing substantive input and recommendations for capacity building initiatives within GFCE. She underscored the Advisory Board's support for the Accra Call, offering strategic advice and direction for its content. Louise also highlighted the diverse and enriching multistakeholder composition of the GFCE AB, representing various backgrounds such as civil society, academia, and the technical community. Lastly, she spotlighted ongoing AB initiatives, including the organization of a Civil Society breakfast during the GC3B, aimed at enhancing civil society engagement and participation in GFCE activities in the future.

Working Group A Session: Evolving National Cybersecurity Strategies

The GFCE Working Groups (WG) convened to converge around thematic lines – fostering collaboration, knowledge sharing, and coordination of efforts. The WG-A session aimed to foster discussion on Evolving National Cybersecurity Strategies, and linked these to the Framework on Responsible State Behaviour. Speakers from the Working Group linked national cybersecurity strategies with threats and opportunities stemming from emerging technologies (AI, quantum computing, etc.)

Background of the session:

Working Group A conducted a dynamic session focusing on the evolution of National Cybersecurity Strategies and introduced the new Chair. The discussion emphasized connecting these strategies to both threats and opportunities arising from emerging technologies such as AI and quantum computing. The panel, moderated during the session, paved the way for a subsequent breakout discussion.

Key activities:

The panel gave representatives the possibility to share their experiences in adapting and adopting a National Cybersecurity Strategy (NCS), from the perspective of authorities in the US, Ghana and Mauritius. Participants were then encouraged to exchange insights and collaboratively brainstorm on how to adapt to developments in the cyber landscape through National Cybersecurity Strategies, while also taking into account the Framework on Responsible State Behavior. Through an interactive breakout discussion, and with the help of three facilitators, participants exchanged ideas on three guiding questions which contributed to important conversations among smaller groups as well as concrete collaborative action points for the Working Group.

Key takeaways:

Participants agreed that current assessment tools and evaluation frameworks to inform cyber capacity building are generally vast and over encompassing. The need for universal baselines and two levels of validation were discussed as approaches that can ensure more accurate evaluations. In terms of the NCS supporting the Framework on Responsible State Behavior, participants highlighted the need to illustrate the benefit of an NCS for the whole of society, and, as an added benefit, to achieve domestic capacity goals. Finally, the Working Group suggested that different approaches to integrate emerging technologies into an NCS could be mapped for insight.

Working Group B Session: Ensuring Resilient Critical Information Infrastructure

The session illustrated the GFCE Working Group B as a dedicated platform for GFCE Members and Partners to converge around specialized topics - fostering collaboration, knowledge sharing, and coordinated efforts.

Background of the session:

The panel discussion offered an opportunity for presenters to share various perspectives on capacities needed for countries to ensure cyber resilience within critical information infrastructure and how to leverage good practices among nations and stakeholders working on this area.
In this interactive session on Ensuring Resilient Critical Information Infrastructure, participants were encouraged to exchange insights and collaboratively brainstorm on priority areas in Critical Information Infrastructure Protection.

With moderation, three panellists working across different regions were introduced to speak on behalf of their countries.

This session provided participants with the opportunity to reconnect in person, exchange knowledge and best practices within a multistakeholder context, and identify areas where the Working Group can direct its efforts in the coming year.

Key activities:

A scene-setting panel on Critical Information Infrastructure hosted three speakers which are actively shaping the field in their respective regions. The session concluded with breakout discussions in a speed dating style, where participants were given the opportunity to discuss guiding questions in smaller groups. The session thereby illustrated diverse efforts in the field, while giving participants the opportunity to listen to their peers, and most notably, shed light on potential areas for the WG to collaborate on for future concrete outputs.

The facilitators prepared questions for participants covering topics such as trust building amongst CSIRTs or information sharing between CIP actors, etc. Participants were encouraged to gather in groups and explore together these questions and report back to the group.

Key takeaways:

The discussions throughout the session led to some key takeaways and action items for WG B. Overall, it was agreed that Critical Information Infrastructure Protection is not an end by itself, but rather the means to an end. As such, every country has the duty to continuously improve its cyber resilience. Here is where knowledge sharing through best practices is crucial and needs to be pursued, encouraging public-private dialogue and communication. Pushing further the idea of best practices, a knowledge-sharing model should be facilitated and established to increase support to developing countries. To support this intent of practice- sharing through expertise, trust building and exercises are to be put in place.

Working Group C Session: Addressing Cybercrime enabled by Emerging Tech

The WG-C session aimed to foster discussion on new and emerging cyber threats as well as good practices on addressing such threats. Speakers from the Working Group covered the role of public and private actors with a focus on the exploitation of emerging tech by cyber criminals.

Background of the session:

In this interactive session on Addressing Cybercrime enabled by Emerging Technologies, participants were encouraged to exchange insights and collaboratively brainstorm on priority areas in cybercrime capacity building. The session fostered discussion on existing and emerging cyber threats including those enabled by AI.

Additionally, it provided participants with the opportunity to exchange knowledge, leverage the multistakeholder community, and identify areas where Working Group C can direct its efforts in the years ahead.

Key activities:

The session was opened by the Working Group C Chair, who proceeded to summarise the work of the WG-C since 2018, which includes, but is not limited to, the Cybil portal, the clearing house mechanism and more recently the WG-A/WG-C collaboration on their webinar series for UN cyber-processes and capacity building. The Chair then opened the floor to the panel, which together reflected on how best to address cybercrime enabled by emerging technologies.

The last activity of the session was a version of speed dating, where three facilitators, prepared questions for participants, who were encouraged to gather in groups and explore some possible answers and solutions to these questions.

Key takeaways:

The session ended with a call to action by the Chair, who urged continued effort in terms of capacity to address cybercrime across both the Global North and Global South. She highlighted the need for WG C to consistently address new issues and topics emerging in the future, to focus on a collective approach, and to further anticipate the threats that may arise from emerging technologies. The session also highlighted the great necessity for Public-Private Partnerships to address cybercrime, and the underlying need to work on information sharing and trust building. Staying within a more global framework, interstate collaboration between law enforcement organizations is essential going forward.

Working Group D Session: Building a Cyber Resilient Culture

Background of the session:

The WG-D session aimed to foster discussion on most pressing skill gaps and priorities as well as good practices from national efforts and campaigns. The focus was on humans as the weakest link and gave Members and Partners opportunities to share good practices, approaches, and efforts to address gaps.

Key activities:

Working Group D Chair hosted the session with a short presentation on the work of the Working Group and a panel of inspiring speakers.

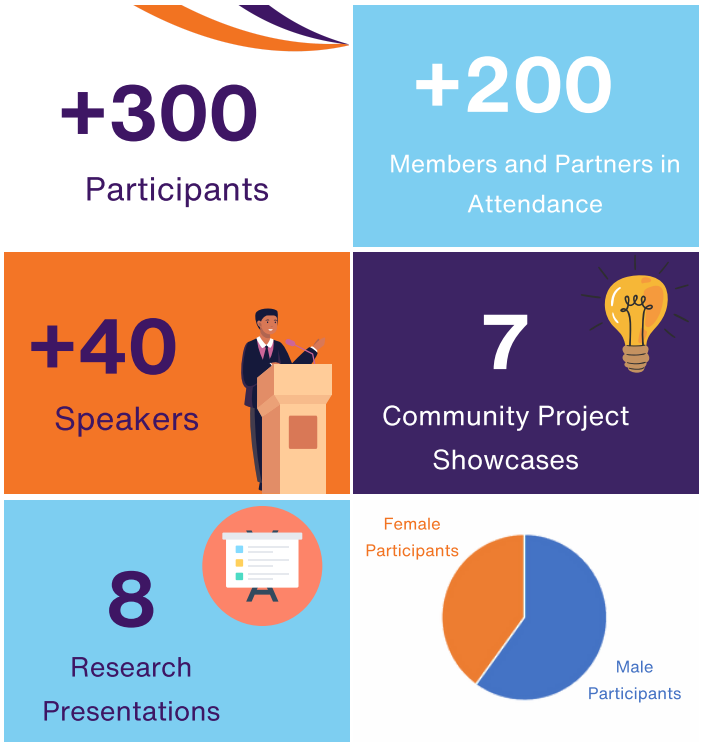
Each speaker illustrated how their work is contributing to building a more cyber resilient culture. More generally, the session connected practitioners and actors within the field of cyber security culture & skills, enabled knowledge exchange, and helped to identify areas where the Working Group could direct its efforts in the future.

The scene-setting panel served as an illustration of efforts in the field across diverse regions and sectors. With the help of three facilitators, participants discussed questions ranging from the most pressing skills gaps or priorities in the cybersecurity workforce to examples of successful Public-Private Partnerships.

Key takeaways:

Within the breakout discussions, concrete ideas on how to leverage what the community is already doing were presented. For example, in the context of enabling a cybersecurity workforce, pathways to enter the market could be mapped and a profile-building exercise could be beneficial to those looking to enter the workforce. A broad range of skills, from technical to non-technical / human skills, are required across the sector. To that end, transferable and other beneficial skills should be leveraged for smoother transition or entrance into the cybersecurity market. Participants agreed that networks and partnerships are beneficial in creating more impact, engagement, and successful results. Therefore, partnerships across sectors can result in gains for all partners involved and generally improved outcomes.

Annual Meeting in Numbers



Contact Us

For more information about GFCE or Annual Meeting sessions or if you have any questions, please reach out to the GFCE Secretariat through our email: contact@thegfce.org

To stay updated about the GFCE projects, activities and initiatives, check out our website and follow us on our social media channels.

@theGFCE

@theGFCE

thegfce.org