GLOBAL FORUM ON CYBER EXPERTISE

GFCE ANNUAL MEETING 2022 REPORT

PREPARED BY THE
GFCE SECRETARIAT

SEPTEMBER 2022

Table of Contents

Report on the GFCE Annual Meeting 2022

Coordination for the Future

The field of cyber capacity building (CCB) is rapidly maturing, a trend that is supported by the mushrooming of actors, projects, initiatives, and networks. The GFCE, as the multi-stakeholder platform for CCB, must evolve to support and address the needs of the Community while reducing fragmentation of efforts. Towards 2023, the GFCE is therefore focused on ***coordination for the future,*** to leverage and streamline existing efforts, avoid duplication, strengthen global cooperation, and foster knowledge sharing. Central to the GFCE's efforts in improving coordination will be i) reinforcing a demand-driven approach through expansion with regional (locally based) liaisons and offices and ii) mobilizing resources for CCB through the organization of the Global Conference on Cyber Capacity Building (GC3B) in 2023.

The GFCE Annual Meeting 2022 in the Hague brought the GFCE Community together in person for the first time in almost three years to reflect on the GFCE's developments and activities, explore the GFCE's coordination role in identified areas (e.g. gender inclusivity, UN processes, regional efforts), and exchange ideas or updates on key topics. In line with previous GFCE Annual Meetings, an open, informal, and interactive setting was established throughout all three days.

DAY 0

On Day 0, structures and committees in the GFCE ecosystem convened in parallel sessions to share updates, discuss the groups' progress, and address important topics that will impact their work for the years ahead. Few of the meetings organized were the GFCE Foundation Board, Friends of Sierra Leone Clearing House Meeting, Working Groups Leadership, GFCE Regional Representatives, the GC3B Steering Committee, the GFCE Strategic Dialogue and the Western Balkans meeting.

DAY 1

On Day 1, plenary and interactive sessions were held to explore the GFCE's developments and way forward. Day 1 highlighted the added value of the GFCE and provided opportunities for Members and Partners to share their own activities, expertise or initiatives. The Secretariat also hosted an informal breakfast for the GFCE Women in Cyber Capacity Building Network.

DAY 2

Day 2 provided opportunities for the GFCE Community to come together in working sessions - an integral feature of GFCE Annual Meetings - to brainstorm and provide input on important topics.

Event Photography

You can use **this link** to see and download photos from the Annual Meeting. **If you share them on social media, don't forget to tag us and use the meeting's hashtag #GFCEAnnualMeeting2022.**

GFCE
Global Forum on Cyber Expertise

GFCE Annual Meeting 2022

Thank you for joining us!

DAY 1

GFCE Community Showcase Hour

In two parallel breakout sessions, GFCE Members and Partners had the opportunity to share their good practices, recent deliverables or new initiatives.

Quad9 Secure and Privacy Proof DNS, Timo Koster (Presentation)	**UN Singapore Cyber Programme, Sithuraj Ponraj, CSA Singapore (Video)**	**Increasing Global Cyber security Talent Through Games, Danielle Santos, NICE (Presentation)**	**Introduction to Table Top Exercises (TTXs), Gerard Elfa García, Capgemini (Presentation)**
Timo presented Quad9, a non-profit foundation providing a free DNS service across the world. Quad9 is dedicated to the cause of universal access to a free and secure internet and provides a maximum security and 100% privacy proof DNS resolver, which in some parts of the world is the only one of its kind.	Sithuraj showcased Singapore's capacity building efforts at the UN through the United Nations Singapore Cyber Programme that includes the UN-Singapore Cyber Fellowship and the Norms Implementation Checklist Workshop.	Danielle talked about the inaugural International Cybersecurity Challenge (ICC), hosted by ENISA, was held in June 2022 in Athens, Greece. Seven teams representing over 60 countries faced off to showcase their cybersecurity skills and compete for the gold.	Gerard presented a GFCE Working Group B initiative on developing a guide for cyber security Table-Top Exercises (TTXs). He provided an update of the work that is being done, the objectives and deliverables of this project.
Africa Cybersecurity Resource Centre (ACRC), Jean-Louis Perrier (Presentation)	**Digital Connectivity and Cybersecurity Partnership (DCCP), Komal Bazaz Smith, DAI (Presentation)**	**G7/ECOWAS Initiative for Cybersecurity, John Reyels, Germany (Presentation)**	**UNIDIR Cyber Policy Portal, Andraz Kastelic (Presentation)**
Jean-Louis presented ACRC, a not-for-profit public private partnership consortium dedicated to improving the cyber resilience of about 3.000 financial institutions in Africa against cyber threats.	Komal presented DCCP's activities aiding countries in: developing state-of-the art, secure and resilient infrastructure improvements; pro-competitive legal and regulatory reforms consistent with market values; policy approaches that facilitate innovation and investment from the U.S. and likeminded countries; and cybersecurity practices in line with international best practices.	John presented a new initiative from G7 and ECOWAS which focuses on strengthening cyber resilience in four action areas: (1) Developing cyber diplomacy skills, (2) Increasing cyber security of critical infrastructure, (3) Fighting cybercrime with a focus on the protection of vulnerable groups online and (4) data sovereignty and data regulation in the West African context.	Andraz presented the Cyber Policy Portal, UNIDIR's confidence-building and research tool, explaining the underlying data collection methodology, new features and the role of the portal in the context of the relevant multilateral processes dedicated to the international ICT security.

'Friends of Congo' Clearing House Meeting

In March 2022, the Republic of Congo submitted a request for support from the Clearing House for: (1) drafting of a National Cyber Security Strategy (NCS), (2) establishment of the country's first governmental CSIRT, and (3) promoting understanding of existing cyber legislation through public outreach campaigns. The meeting gathered together relevant stakeholders to discuss the request and define next steps for supporting the Republic of Congo.

First, ***Eric Armel N'Doumba*** from the Ministry of Posts, Telecommunications and the Digital Economy of the Republic of Congo, presented the country's current cyber security landscape which focuses on the development of the digital economy, innovation, technological and scientific research. Amongst other topics, the country is striving to enhance cyber diplomacy capacity and has recently received support funds for the realization of the CSIRT.

Participants gave their perspectives in relation to the Clearing House request, highlighting that it is greatly important for the country to first do an assessment of the needs and offers and create a roadmap of the technical and financial support needed. Additionally, stakeholders offered their support to assist the country with risk assessment planning and by sharing experience on how they have supported other countries with similar needs. The GFCE Secretariat will play the coordinating role between the Republic of Congo and relevant stakeholders who will be involved in supporting this Clearing House request.

Working Group E Side-Meeting: Exploring Scope and Focus

The side meeting on Working Group E brought together representatives from different stakeholder groups, including government, private sector and the technical community to discuss the proposed way forward for Working Group E on Cyber Security Internet Standards. Following consultations with the GFCE Community earlier this year, the resulting proposal was to continue developing the established Triple-I project as well as redesign the former WG-E to incorporate two focus tracks (Technology and Standards), that will further be developed by two interest groups.

The GFCE Triple-I initiative helps safeguard and promote a robust, transparent and resilient Internet infrastructure. It seeks to deepen and broaden the expertise in locally applying, testing and monitoring compliance with widely agreed open internet standards. Participants highlighted the need to extend the implementation and compliance of cyber security standards, as well as the importance to have better awareness and understanding regarding the different frameworks that exist on internet standards, especially on a regional level. Another point raised by the participants was the importance of understanding the cyber threats landscape and the consideration for the GFCE to develop a cross-organizational annual threats assessment report and to raise awareness on standards within the GFCE Community.

Opening Ceremony of the Annual Meeting 2022

The GFCE Annual Meeting 2022 opened with welcome remarks from Chris Painter, President of the GFCE Foundation Board, the GFCE co-Chairs, Maartje Peters on behalf of The Netherlands and Alkesh Kumar Sharma, the new co-Chair on behalf of India and Rick Harris, co-Chair of the GFCE Advisory Board 2022-2024.

First ***Marjo Baayen, GFCE Secretariat Director,*** opened the meeting giving a warm welcome to all participants, expressing how great it is for the GFCE Community to be able to meet again in-person, to network and share experiences, and learn from each other.

Maartje Peters, was appointed as the GFCE co-Chair on behalf of The Netherlands in 2021. In Maartje's opening remarks, she underlined the GFCE's unique position as an important cooperation mechanism for CCB that connects needs, resources and expertise and makes practical knowledge available to the global community. The GFCE's impact is made by its Members and Partners through facilitation via its Working Groups, regional coordination, Cybil, Clearing House, Research Agenda, and its various committees, meetings and events. Therefore, the impact that the GFCE makes in CCB is closely linked to the successes and achievements of its Community. Maartje highlighted that the GFCE's vision of a free, open, peaceful and secure digital world resonates deeply with the Netherlands, sharing the view that, in order to effectively strengthen CCB, a multi-stakeholder approach is necessary.

Shri Alkesh Kumar Sharma, was announced as the new GFCE co-Chair on behalf of India. Shri Alkesh highlighted the GFCE's demand-driven approach and regional focus, bringing concrete examples of how the GFCE's activities align with India's developments when it comes to cyberspace and capacity building. As mentioned, in 2022-2024 the GFCE will focus on global cooperation, regional coordination and local collaboration and thus the platform is well-positioned to leverage capacity building through connecting regional with global stakeholders, identify needs and share available expertise. Shri Alkesh reaffirmed India's position closely connected with the GFCE in creating a safe and secure cyberspace, where everyone should be able to fully receive the benefits of ICT.

Rick Harris presented the new GFCE Advisory Board 2022-2024 and explained that the board is an advocate for the civil society within the GFCE Community and it advices on the strategic direction of the GFCE and its way forward.

Keynote on Cyber Capacity Building in Africa

Following the opening session, ***Dr. Towela Nyirenda-Jere from AUDA-NEPAD*** provided a keynote on CCB efforts and developments in Africa.

Dr. Towela explained that through the African Union Commission, Regional Economic Communities (RECs) and other regional institutions, Africa has over the years put in place various strategies, policy frameworks and initiatives towards the attainment of digital economies aligned to the Digital Transformation Strategy for Africa. Despite the immense progress, it is also clear that Africa is not sufficiently equipped or capacitated to deal with cyber issues and thus, it is crucial for African countries and organizations to have in place effective strategies and programmes related to cyber capacity building.

As an example of such programs, she highlighted the implementation of the **AU-GFCE Collaboration Project** aimed to enable African countries to identify and address their cyber capacity needs and strengthen their cyber resilience. As mentioned, key principles in the implementation of the project have been ownership and inclusiveness; all 55 AU Member States were invited and participated in the development of the project and 35 Member States have appointed designated Focal Points, making up the Africa Cyber Experts (ACE) Community. The Cyber Capacity Building Coordination Committee was also established comprising of African organizations and is chaired by AUDA-NEPAD.

GFCE Updates and Developments

The aim of the session was to update the GFCE Community on how the GFCE and its ecosystem have evolved over the past year. The session further explained the GFCE's strategic ambitions for 2023-2024, specifically highlighting the importance of the regional approach, and how this will support the

GFCE Community with their cyber capacity need and efforts. A presentation was given by ***David van Duren (GFCE Secretariat Director).***

David started by highlighting how the GFCE has evolved starting with a supply-driven approach back in 2015 by establishing and enlarging the GFCE Community and building its ecosystem based on the available knowledge and expertise through the endorsement of the **Delhi Communiqué** on a GFCE Global Agenda for Cyber Capacity Building and the establishment of the Working Groups. Over the past years, the GFCE has been striving to transition to a more demand-driven approach by prioritizing countries' needs and offering tailor-made support. Examples include the GFCE Clearing House and the AU-GFCE Collaboration Project. He stressed that the GFCE exists for its community and to support the facilitation of CCB projects of its community.

This was the main reason for the establishment of the regional hubs that can help prioritize the regional and national needs. Namely, the Community can use the GFCE within their projects by getting in touch with the regional community. For example, in Africa, the GFCE has established its Africa Cyber Experts (ACE) Community. Getting in touch with the community can improve the efficiency of projects and avoid the duplication of efforts. Additionally, it will support local ownership and will connect to existing regional activities and efforts to reduce the overlap with other stakeholders. Another added value is to increase the project sustainability and share and learn from past experiences from the community to improve the CCB support.

David invited the Community to provide more feedback on the **GFCE CCB Strategic document 2022-2024.** All in all, the GFCE aims to strengthen coordination in the future to improve both the sustainability of the community's CCB efforts and to ensure a demand-driven approach.

Private Sector Perspective: What States should know on technical developments and their impact on Cyber Capacity Building efforts

The increased reliance on technology over the past two years has resulted not only in an acceleration of technical developments, but also of accompanying risks. With the public-private sector becoming more interwoven, the private sector's role in CCB is becoming increasingly prominent and complex. This session introduced key technical developments and associated threats, forming a panel discussion with ***Eben Louw (IBM), Nikolas Ott (Microsoft), Tim Appleby (Mandiant)*** moderated by ***Olivia Blackmon (DAI).***

Olivia Blackmon highlighted the importance of addressing areas such as countering hybrid threats, disinformation, and the integrity and protection of critical infrastructure and cybersecurity. Recently, attacks have become more sophisticated and targeted and that is the reason why greater coordination is needed, with an integrated national and regional approach on emerging technologies and a specific focus to increase digitalized societies.

First, ***Eben Louw*** highlighted that one common technical trend identified today comes from an incident response point of view, with countries and companies not having the necessary technologies to adequately respond to attacks. One aspect to this, is the need to constantly train people to know how to use the new technologies and implement the right processes. Eben added that it is necessary, from a security perspective, for the right technologies to be in place and configured correctly to make sure that no vulnerabilities are set aside, and things are looked at from a holistic security-focused point of view.

Nikolas Ott mentioned that as we live in a transformational phase, we need to think how teams can collaborate on cross-cutting issues with emerging technologies, as threats and changes affect societies as a whole and not just the organization under attack. As highlighted, when building an ecosystem, it is foundational to understand what needs, threats and challenges exist. With recent attacks globally, the understanding of cyber resilience is changing; it is important for societies to think how to leverage new technological features to protect critical infrastructure and set in place regular trainings for those involved to understand the constant changes across sectors and regions.

Tim Appleby explained that the overall trend is for a paradigm to occur every decade, and today we have shifted towards a 'Zero-Trust' approach, which secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction. As mentioned, organizations are currently facing many challenges, thus, it is important to set in place the right architecture which should match the skills and workforce of those implementing it.

All panelists agreed that involving the private sector more in the GFCE will benefit the whole Community as pieces that help build a more resilient environment will come together in an easier way. Within the GFCE, the knowledge and expertise of the private sector can be key for organizations to stay up to date on the latest technological developments and threats.

Global Conference on Cyber Capacity Building (GC3B): Strengthening Cyber Resilience for Development

The Global Conference on Cyber Capacity Building (GC3B) will be a key gathering to secure and improve decision makers' awareness on cyber capacity building, strengthen coordination of efforts on a global scale and widen the pool of resources available. The 2023 conference will focus on "Cyber Resilience for Development" as a central theme. This panel session presented the concept and aims of the Conference and highlight the opportunities for global cooperation through the GC3B, namely on bridging the CCB and development communities together. The panel was comprised of ***Chris Painter (GFCE), Anat Lewin (World Bank), Stephane Duguin (CyberPeace Institute), Tal Goldstein (World Economic Forum),*** moderated by ***Francesca Spidalieri (GC3B Program Team).***

All speakers highlighted the interconnection between the development community and the cybersecurity community, and the importance of elevating and mainstreaming cyber resilience and CCB into the international development agenda, which is the main aim of the Global Conference on Cyber Capacity Building (GC3B).

Chris Painter stated that the GC3B is important for the GFCE Community because it catalyzes global action towards elevating the importance of CCB and supports the implementation of the GFCE Strategy. Chris highlighted the synergies between the GC3B and the GFCE's strategy for 2022 onwards, noting that the GFCE's ambitions under global cooperation align with many outcomes and objectives of the conference such as enhancing private sector participation, building a strong civil society network, mainstreaming gender in CCB, connecting CCB with the development community, increasing the GFCE's external engagement in relevant cyber dialogues, and establishing a global CCB agenda.

Anat Lewin stressed that cyber resilience and CCB are crucial to the work of the World Bank in developing countries, highlighting the importance of protecting platforms, services and infrastructures that are transforming digitally, to secure and safeguard global investments. She also affirmed that the

international cybersecurity community can work together to achieve this by strengthening coordination and increase the volume of cyber experts, especially in developing countries.

Stéphane Duguin underlined that the GC3B will help strengthen the multi-stakeholder, demand-driven approach to international development to better serve the priorities of developing countries. He identified the importance of understanding that cybersecurity is not only associated to the digital world, but it affects public services as well. Hence, it is important to measure the human impact of cyber-attacks in order to assess their consequences, which can only be achieved with the active participation of civil society and other multi-stakeholders.

Tal Goldstein emphasized the importance of the private sector within cybersecurity and the need to think about how to bring them to the table, how they can be involved, and understand what it means for the private sector to walk in the cybersecurity and CCB realm. He stated that the private sector's involvement will foster greater coherence and coordination for CCB activities and help expand the pool of resources available for equitable, sustainable, and demand-driven cyber resilience for development. The date and location of the GC3B will be announced in the coming weeks.

Ensuring Gender Sensitive Approaches and Inclusivity in Cyber Capacity Building

The past year the GFCE has worked on prioritizing mainstreaming gender in CCB within the ecosystem, through a series of recommendations and actions with the input and support of the GFCE Community. This session focused on discussing the beforementioned topic and highlighted a number of initiatives focused on gender-sensitive approaches and inclusivity in CCB. A panel discussion included ***Dr. Towela Nyirenda-Jere (AUDA-NEPAD), Craig Gillies (Australia), Cherie Lagakali (GFCE Pacific Hub)*** with moderator ***Louise-Marie Hurel (Igarapé Institute/GFCE Advisory Board).***

Louise-Marie Hurel opened the session by highlighting that more and more organizations today have started incorporating gender considerations with programs and research in their working activities and one of the critical questions to address is how we can ensure to raise awareness globally on the importance of gender in cyber security. Louise-Marie asked the panelists to reflect on how their respective organization/country has included gender in the CCB agenda.

Dr. Towela Nyirenda-Jere mentioned that today, although we all understand the need for inclusivity in cyber security, the focus should be given more on meaningful engagement, impact and empowerment. She raised the point that when talking about inclusivity in cyber, we need to think of everyone who is accessing the information society, starting from young children who should be able to protect themselves online. We also need to make sure we are not marginalizing certain segments of the population because of the way we are structuring the inclusivity considerations.

Cherie Lagakali, shared that in the Pacific, it has not always being easy for everyone to understand that equality in leadership positions in the professional environment is a must. As highlighted, women in the region have the need for informal mentorship, being able to connect with each other and especially with broader global networks such as the GFCE Women in Cyber Capacity Building Network. She also highlighted the importance of having structured programs to encourage the participation of more and more women from the region in high-level negotiations, for example the Women and International Security in Cyberspace fellowship initiative.

Craig Gillies shared more information on how Australia is supporting the fellowship initiative, bringing women from the Indo-Pacific region to the UN Open-Ended Working Group (OEWG) and Ad-Hoc Committee on Cybercrime (AHC) negotiations, mentioning that in the last OEWG 52% of the interventions were made by women. In the Indo-Pacific region, although the gap between women and men who have access to the internet is shrinking, that is not reflected in the context of cyber literacy rights, cyber security workforce, online content and culture. Craig mentioned that Australia is focusing on GEDSI (Gender, Equality, Disability and Social Inclusion) mainstreaming programs and highlighted that one of the first things to do to mainstream gender is to acknowledge that it is an actual problem, make a plan and commit to do something about it.

In conclusion, panelists highlighted the challenge of getting more partners involved in this topic as many organizations have very complicated structures and processes and it is difficult train and educate these businesses in expanding their work, as well as translating research already done in this field into tangible goals for future work to be made in closing the gender gap.

Confidence Building Measures (CBMs) Implementations and Capacity Building

This session discussed confidence building measures (CBMs), looking in particular at how CBMs are being addressed in the context of international security and at the linkages with capacity building. Additionally, panelists explored how the GFCE can leverage its network and ecosystem for greater awareness raising and coordination. The panel discussion included ***Craig Gillies (Australia), Szilvia Toth (OSCE), Daniela Ruiz Dominguez (Mexico), Arthur David (Canada), Sithuraj Ponraj (CSA Singapore),*** moderated by ***John Reyels (Germany).***

Discussions on confidence building measures (CBMs) in the context of international security in the use of ICTs are taking place as part of a diplomatic process ongoing within the United Nations. The Open-Ended Working Group (OEWG) in the UN First Committee is the main working group dealing with cybersecurity issues, with the aim of advancing stability and responsible state behaviour in cyberspace.

Seen from this perspective, the primary aim of CBMs is to build trust and reduce the potential for conflict between states. Given the increasing complexity of cyberspace and the threat landscape, the potential for misunderstanding and escalation of conflict is a real risk. Confidence building measures help to establish communication channels between states and ensure a baseline level of transparency. Typically, the realities of the UN as a forum for multilateral negotiation have meant that reaching consensus can be challenging. The establishment of confidence building measures at the international level is therefore seen as one of the success stories resulting from the OEWG.

This is a particularly noteworthy effort because it provides a clear example of how states can bridge divides across differing interests and priorities in the context of international security. It has also helped to create momentum for information sharing around action-oriented initiatives and builds on efforts in the previous OEWG and Group of Governmental Experts (GGE) to create a template that can be followed by others. A total of seven CBMs have been developed between 2018-2021 under the OEWG, with many of these now beginning to be adopted. Whilst the development of CBMs is a process that takes place largely between states, there is a strong need to ensure that implementation involves and is reflective of multistakeholder perspectives.

A major challenge going forward is the need to demystify CBMs, helping states to understand what needs to be done and encouraging the involvement of other stakeholders to assist with implementation. Subscribing to the standards outlined by a CBM are just the beginning. Many small and developing states in particular find it challenging to reach the operational, technical, and policy requirements related to cybersecurity CBMs. As such, many have recognized that capacity building will be foundational to enabling implementation of commitments in this area.

Within the OEWG, a group of like-minded countries from different parts of the world have come together to advance the establishment of a strong institutional mechanism for confidence building measures. This effort has been greatly informed by and draws on the work of the Organization for Security and Cooperation in Europe (OSCE) and Organization of American States (OAS).

Practical guidance highlighting how CBMs can be developed, maintained and implemented at the national and regional levels already exist. For example, in partnership with industry and civil society, Singapore and other ASEAN states created a norms implementation checklist, indicating the processes and capabilities. The OSCE has also released best practices on the development and maintenance of points of contact networks and has developed e-learnings based on experiences.

For some, building trust also involves looking at the operational aspects of CBMs and understanding the prerequisites and contingencies involved in implementation. For example, for some CBMs to work in practice it is crucial to have knowledge on who and where capabilities are located. One thing that would be helpful here is more transparency from states on what their declared cyber capabilities are. These examples underline the need for further input at the multilateral level, helping to develop further guidance and encourage more engagement between states but also with other stakeholders. Advancing voluntary & non-binding measures by all UN Member States remains the goal and a shared responsibility.

DAY 2

Roundtable Work Session 1: Strengthening Collaboration in the GFCE Community

On Day 1 of the Annual Meeting, the GFCE's developments and strategic ambitions were outlined, including on emerging topics and important processes related to CCB. Participants brainstormed and discussed in a roundtable setting, how to strengthen collaboration in the ecosystem, with a dual focus: global cooperation and regional efforts.

Using the GFCE collaboration mechanisms and tools as a guideline, participants were tasked with assessing how the GFCE might adapt to keep pace with trends and developments in international CCB. Responding to guiding questions, they were asked to assess the GFCE's role when it comes to a regional approach and global cooperation for CCB.

On the issue of global cooperation, specific focus was placed on engagement in the United Nations Open Ended Working Group (OEWG) and Ad-Hoc Committee on Cybercrime (AHC). It was agreed that capacity building is a prerequisite for the development and implementation of international frameworks. Whilst they should be treated as distinct processes, capacity building should be positioned closely with the norms and standards promulgated in the OEWG and AHC. Besides visibility, the GFCE can play a role in these efforts, for instance by providing guidance on how capacity building is connected to the two processes or by organizing side meetings and workshops around events. These would be informative for all stakeholders and could provide educative value in ensuring that key actors, particularly diplomats, understand the technical foundations of the negotiations. Targeted training should also be developed to assist with implementation of the outcomes of these processes. Specific communities, such as those established in the GFCE Working Groups, could serve as a forum for more concerted information sharing around different aspects of the processes, discussion and consultation on issues on which the GFCE can or should be engaging, and for highlighting the resources and best practices that the GFCE Community has to offer.

On the issue of regional cooperation, a shift to a regional approach was seen as a positive, especially where it leads to increased collaboration and engagement of local stakeholders. It should also lead to the development of more tailored capacity building efforts. Thinking about regional collaboration in terms of a top-down approach as a first step is useful for identifying which organizations and communities should be involved, and what the frameworks are for cooperation. Sub-regional cooperation is also key for ensuring cohesion and avoiding fragmentation, as these groupings are often more aligned in social and economic terms. Further, the need for information sharing between regions still exists particularly as they face similar vulnerabilities and threats, so it is a challenge to find ways to ensure communication and information sharing between regional initiatives. It was recommended that the hubs focus initially on engagement with stakeholders to understand what the particularities of the region require in terms of capacity building, and to help develop awareness on what is already available. The hubs could also explore and pioneer ways of utilizing the Cybil portal and research agenda towards these aims. The outputs of GFCE Working Groups could also be geared towards regional efforts. The discussion placed importance in the outcomes of the regional approach. More data and information are needed on what is happening on the ground so that guidance can be developed on how to tackle common or specific challenges. Regional hubs could serve as operational knowledge centres, helping to bridge divides between the local, regional and global levels.

The GFCE's Regional Efforts

Since 2020, the GFCE has placed increasing emphasis on adopting a regional focus while highlighting the need for a demand-driven approach to CCB. During this session, participants learned more about the GFCE's efforts and developments in Africa, Latin America and the Caribbean (LAC), Southeast Asia, the Pacific, and Western Balkans (Europe). Following a panel discussion, participants continued in breakout rooms to delve deeper on one of the above-mentioned regions of interest.

Western Balkans Region

The Regional Breakout session on the Western Balkans built on discussions initiated by the GFCE and various key actors, amongst donors, implementors and recipient countries, with the aim to further the exchanges on CCB needs of countries and explore ways in which the GFCE Community can better serve the region. Discussions in this session were preceded by interventions from panellists ***Vladimir Radunovic (Diplo Foundation), Silja-Madli Ossip (EU CyberNet), Artan Dreshaj (Kosovo*), Ilija Zhupanoski (North Macedonia)*** and ***Bruce McConnell (ORF America).***

Bruce McConnell reflected on the strategical importance of the region, increased by the recent escalation in cyber-attacks in the region. ***Vladimir Radunovic*** underlined that these recent developments were set against a background of complex relationships between countries, the already significant presence of donors and implementors on the ground, and the accelerated digitalisation not supported by an increase in cybersecurity.

Silja-Madli Ossip underlined that Western Balkans were at the centre of EU's attention already through the EU Cybersecurity strategy and informed of the EU CyberNet mapping of EU funded and member states funded CCB efforts around the world. ***Bruce McConnell*** presented the conclusions of a two-day coordination meeting in Skopje on the topics: cyber-defence, cyber-resilience, cybercrime and information disorder. The overall conclusion points to the need to advance beyond collaboration to synergies, maintain connections and build on partners' initiatives. In this context, ORF America would welcome the GFCE taking up a role in further stakeholders' coordination. ***Artan Dreshaj*** underlined the regional and national cyber challenges met, noting the GFCE could provide a welcome, neutral forum to support regional cooperation. ***Ilija Zhupanoski*** mentioned the shift in focus of high-level political leadership to the necessity to fast-track cybersecurity matters and protecting critical infrastructure.

On the challenges and concrete steps for furthering CCB coordination in the region, ***Bruce McConnell*** proposed that donor(s) could take up the convener role for donor coordination. ***Vladimir Radunovic*** presented the internal coordination model in Serbia of a network gathering private sector, government, NGOs, meeting at least once a year to update each other on their activities, focusing on different topics: awareness raising, cyber skills, education. ***Silja-Madli Ossip*** reminded the group of the assessment study produced by e-Governance Academy that provides recommendations for priorities and concrete measures for more effective CCB in the region. ***Artan Dreshaj*** noted the good cooperation with OSCE, DCAF, USAID. ***Ilija Zhupanoski*** proposed the model and extending the membership of the Open Balkans Initiative (Serbia, North Macedonia, Albania), where topics of cooperation are first discussed at high-over political level, then taken up at working, institutional level, through regular meetings and coordination.

Milan Sekuloski (DAI) underlined that the stringent need is for coordination of donors, whilst national coordination does take place in different formats and proposed for the region to come together in neutral formats, such as GFCE and FIRST. Further, ***Szilvia Toth (OSCE)*** underlined that the OSCE has

missions in all Western Balkans countries (except Kosovo*) and an informal working group in place as venue for cooperation, addressing also updates in implementation of the CBMs, which could be a platform for further discussions. ***Olivia Blackmon (DAI)*** added to the calls for increasing donor coordination in the region and stressed that a regional approach should be maintained on issues such as critical risk and response monitoring – potentially through a coordinated sharing network. In this sense, the GFCE was considered a good convener for such a network. ***Bert Theuermann (Austria)*** and ***Szilvia Toth (OSCE)*** additionally stressed the need for Western Balkan countries to be supported to engage with the UN cyber processes. ***Péter Horváth (Hungary)*** also noted the importance of fast-tracking cyber process and of Western Balkans region in general.

The session concluded with a consensus on keeping the momentum of the dialogue with main stakeholders in the Western Balkans region for exploring the ways to further the coordination of CCB efforts.

APAC Region

The APAC breakout discussion was moderated by ***Cherie Lagakali (GFCE Pacific Hub),*** with regional representatives on the panel: ***Saia Vaipuna (GFCE Pacific Hub), Klée Aiken (FIRST), Sithuraj Ponraj (CSA Singapore), Steven Matainaho (Papua New Guinea) and Malison Phommavichith (Lao PDR).***

The GFCE Pacific hub was recently established in the region and the other soon-to-be GFCE hub that will be linked with the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) will follow. The panelists discussed how the agenda of the hubs will be shaped and certain challenges that are identified in the APAC region.

As highlighted by ***Saia Vaipuna***, the GFCE Pacific hub is unique as it is not embedded in an existing network or organization. This factor creates a big challenge as the Pacific team needs to focus first on building relationships in the region. The aim is for the hub to be the first point of call for the Pacific countries as well as key stakeholders when it comes to cyber capacity building. ***Steven Matainaho*** then brought examples by Papua New Guinea, mentioning that for the Pacific, connectivity is still a huge development challenge and while developing ICT, cyber security is not included in the development agenda. The GFCE thus, can provide an opportunity for raising awareness, sharing experiences and learn from others.

Sithuraj Ponraj talked about the future GFCE hub in Southeast Asia which will be connected to the ASCCE. He mentioned that during the Singapore International Cyber Week (SICW), the GFCE will host the second Southeast Asia Regional Meeting, during which GFCE Community and ASEAN stakeholders will come together to identify opportunities and challenges for CCB in the region. More information on the event can be found **here.**

All speakers agreed that the GFCE regional hubs provide an excellent opportunity to connect with the regional and local stakeholders and can be a bridge to the senior officials with the political agenda and the operational experts that do CCB on the ground. The hubs can provide a persistent presence in the region through building long-lasting networks and identifying regional needs, challenges and gaps in regional CCB.

As brought up by the participants the GFCE can do more on the issue of ransomware and cryptocurrency, linking these upcoming issues with CCB. Klée as the new GFCE Working Group B Incident Management & Infrastructure Protection Chair proposed they get together and draft a joint proposal for Working Group B and C on Cybercrime to take forward, also exploring how to connect this project idea with the GFCE Pacific hub.

Latin America & The Caribbean Region

The LAC breakout discussion was moderated by Tereza Horejsova (GFCE Secretariat) and featured a panel with ***Valentina Name (Organization of American States), Robert Collett (Cybil Portal Team), Cesar Moliné (Latin America and Caribbean Cyber Competence Centre) and Pablo Andrés Castro Hermosilla (Chile).***

Valentina Name presented the OAS's cybersecurity program which has three focuses: policy development (assisting member states in developing national cybersecurity strategies), capacity building (helps establish national CSIRTs), research and awareness raising (develops technical documents, toolkits and reports to guide policymakers). The OAS is working on an initiative addressing the gender gap in the cybersecurity agenda with: gender-sensitive standards, strengthening women's leadership and participation in the workforce and increasing awareness of internet users. The OAS also serves as the GFCE Hub in the region and it was announced that the next regional meeting will take place in the Dominican Republic on 14 November 2022. More information on the event can be found here.

Robert Collett introduced the Cybil Knowledge Portal and explained how in the last months, the Cybil team has collaborated with key actors in the region to update their projects on the repository. In the LAC region, there is a trend of the concentration of projects in specific countries; a total of 18 ongoing projects exist in Colombia, Argentina, Mexico, Brazil and other countries. Robert highlighted that it is important to focus on identifying more projects in the region and ways of updating project information on Cybil more regularly.

Cesar Moliné presented the Latin America and Caribbean Cyber Competence Centre (LAC4), implemented by EU Cybernet which is a training facility that develops and provides technical, policy and strategic trainings and works as a channel to CCB projects and training modules developed in the EU. Cesar mentioned that they have hosted the first ever Caribbean cyber security exercise to define, specify and exercise the role of the National Cybersecurity Council in cyber crisis. LAC4 is also co-organizing together with OAS and the GFCE the upcoming GFCE LAC Regional Meeting in the Dominican Republic.

Pablo Andrés Castro Hermosilla brought the Chilean cybersecurity perspective, highlighting that in the LAC region, countries have very different cyber security maturity levels, which is a great challenge. As mentioned, cyber diplomacy is crucial and 4 out of 6 CBMs established in the region are connected to this theme. Another challenge for the region is ransomware, as it has become very complex and recent cyber incidents have proved that it is very difficult for all countries to be able to respond to attacks on time. He highlighted that with many different actors in the region it is very important to identify how things are done and how to better coordinate them.

Participants also pointed out the importance of identifying regional actors who work on similar issues on CCB and connect. Information and knowledge sharing are crucial and that is where the GFCE-OAS

Hub can play a huge role by coordinating existing efforts and leverage those in other regions. It is thus important for the Hub to build its CCB regional agenda and to what a clear image of what this region needs and what CCB entails for it.

Africa Region

The Africa breakout discussion was moderated by ***Velimir Radicevic (GFCE Secretariat),*** with panelists ***Enrico Calandro (Cyber4Dev), Martin Koyabe (GFCE Africa Program Team), Dr. Towela Nyirenda-Jere (AUDA-NEPAD), David van Duren (GFCE Secretariat) and Jaqueline Pateguana (GFCE Secretariat).***

David van Duren started by explaining that the GFCE established the regional hubs, to address the clear gap in understanding the CCB needs at a regional level while maintaining a global perspective. At a regional level, the GFCE aims to contribute to making regional projects more efficient and more effective. To do so, three components were highlighted as being foundational: building a long-lasting CCB community, strengthening the demand-driven approach and facilitating regional needs.

Dr. Towela Nyirenda-Jere highlighted that the African continent has seen a growth of CCB projects which has meant that organizations are now very active in developing policy frameworks and guidelines. Capacity development is being approach in different ways and a lot of the technical development is event-driven through trainings, workshops and other events. Towela also mentioned that the area to pay more attention is on the policy makers and government officials; how do we ensure that they are reached with the knowledge they need to be able to make sure that national development is moving in the right way.

Martin Koyabe shared more information on the AU-GFCE Collaboration project findings. The project first examined the CCB priorities and challenges of African countries. The challenges varied a lot as countries are not on the same level of cyber maturity across different topics such as cyber awareness, skills development, legislation, and other issues. The project also looked at the sustainment and having countries being the owners of CCB projects. Martin mentioned that the findings of the project and experiences will be used to guide the agenda of the GFCE Africa Hub.

Jaqueline Pateguana presented the GFCE Clearing House tool, the match-making mechanism in bringing together requests of CCB assistance from countries with offers for support. It was highlighted that the focus is given in identifying what exists in the GFCE Community on initiatives and projects and connect the dots with others who have similar developments. The aim is to leverage the existing knowledge with others who are in need of it, and find tailor-made solutions for members who need cyber capacity and expertise assistance.

Enrico Calandro presented Cyber4Dev which operates across three regions in the Global South, including Africa. Countries are supported through three pillars: drafting and implementation of national cyber policy, building capabilities on operational and technical level and fostering a network of cyber experts. The focus is also given on cross-cutting issues such as gender and human rights. Enrico highlighted that Cyber4dev has two main objectives: sustainability of the interventions and long-lasting results. To achieve this, the project focuses on empowerment, inclusion, diversity and human rights.

Roundtable Work Session 2: Global Conference on Cyber Capacity Building (GC3B)

The aim of this roundtable work session was to ask for input from the GFCE Community on various aspects of the GC3B, in order to ensure that it has global multistakeholder ownership. This session was the first of several upcoming consultation sessions with the global community and it served as an opportunity to provide input on the conference outcomes and draft program.

Daniel McMurray, GC3B Conference Lead gave a presentation explaining the GC3B aim which is to elevate and mainstream cyber resilience and capacity building in the international development agenda and in national development plans and investments, as key enablers of sustainable development, inclusive economic growth, and social prosperity for all. Additionally, he outlined that the conference is structured around four thematic pillars: (1) Making International Development Cyber Resilient, (2) Collaborating to Secure the Digital Ecosystem, (3) Cyber Capacity Building for the Stability and Security of the Digital Environment, and (4) Operationalizing solutions which is a horizontal, cross-cutting pillar focused on practical solutions that can be of immediate use by practitioners working at the intersection of cyber resilience and international development.

Afterwards, gathered at roundtables in groups of 8-10, participants discussed four discussion questions and wrote their feedback for the GC3B co-organizers to review.

1. One of the objectives of the GC3B is to secure high-level awareness on CCB. High-level attendance is therefore crucial. How can the Conference secure high-level participation?
2. Does the pillar framework capture the topics you would want to discuss at the conference?
3. Who would you like to hear from as a keynote speaker?
4. Which international events do you suggest the organisers use as consultation opportunities?

On the question of how the GC3B can secure high-level attendance, the following suggestions were made: pitch projects that highlight the importance of cyber resilience to VIPs in order to convince them of its importance; partner with regional bodies to facilitate interest from regional leaders and ministers in the conference; align the conference with other large events such as a UN event to economize on the time that high-level ministers have to attend events; avoid patronising language or 'talking down' to the development community; and promoting cybersecurity capacity building as an investment protection for development assistance as a key selling point.

On the question of if the GC3B program pillar framework captures the important topics, participants made the following comments: the suggested topics are comprehensive and the overall pillar structure is great; language of the pillars and topics should be carefully curated to ensure language is not too vague but also not too technical; topics such as the involvement of women and youth, particularly on the leadership level, should be more integrated; topics could focus more on locally-built ecosystems and home-grown solutions; and capacity building should be made long-term with a focus on deliverables and outcomes to ensure sustainability of progress.

Closing Ceremony of the Annual Meeting 2022

After three days of fruitful discussions, interactive sessions and more, Chris Painter gave the closing remarks highlighting that the past few days have shown that capacity building is a fluid concept, requiring a flexible approach that fully takes account of diverse needs and challenges across the design and delivery of initiatives. The Annual Meeting welcomed over 220 participants in-person with more than 100 following the sessions online each day. More than 110 different organizations were represented including 16 new GFCE Members & Partners.

The Annual Meeting has shown the added value of the GFCE Community as a convening platform for advocating CCB. Chris highlighted that the GFCE's ambitions and direction over the coming years will involve building strong partnerships and engagements will all stakeholders. The Community plays the strongest role in moving forward and guiding the strategic direction of the GFCE, especially in relation with the GFCE's external engagement with the UN processes as well as its regional efforts. An important milestone for the GFCE will be the Global Conference on Cyber Capacity Building (GC3B), for which the Community's input was crucial for achieving the conference's objectives and further development of the program.

As the GFCE grows and develops, its approach to supporting demand-driven needs space and locally owned capacity building and it is important to continue strengthen our communication across the platform. The GFCE Community will continue being involved in all stages of the process, something that provides the GFCE with a challenge but also gives an exciting vision for us to work on. In the coming months, the GFCE is planning plenty of opportunities to interact and engage with the GFCE team on a regional level through the GFCE Regional Hubs. The GFCE is increasingly committed and well-positioned to continue supporting and strengthening demand-driven and needs-based delivery of capacity building.

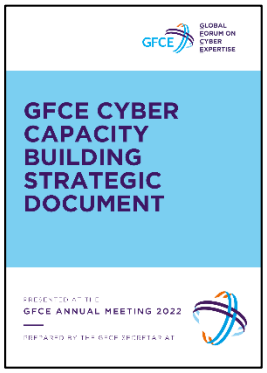
GFCE Deliverables presented at the Annual Meeting 2022

Mid-Year Review 2022

In 2022, the GFCE continues to bridge the gap between CCB demand and supply, focusing on three priority areas: strengthening the demand-driven approach, strengthening regional coordination and maturing to an integrated GFCE ecosystem. The Mid-Year Review 2022 provides a short update on the GFCE's developments throughout this year regarding the GFCE Working Groups, the GFCE Toolbox, the collaboration projects, the regional updates, and other developments regarding the GFCE Ecosystem and Community. Read here.

Global Cyber Expertise Magazine

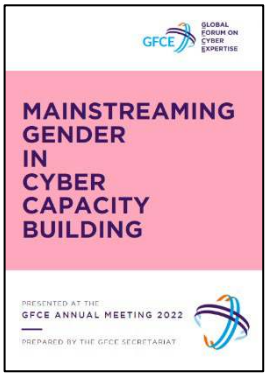
The 11th issue of Global Cyber Expertise Magazine covers a range of topics on cybersecurity, with articles about the latest developments on CCB from each of the four regions (Europe, Asia & Pacific, Americas and Africa). Topics covered in this issue include the Global Conference on Cyber Capacity Building (GC3B) 2023, the cybersecurity foray to deliver the professional shortage in Latin America and the Caribbean, the Digital Access Programme, the Africa Cyber Capacity Building Coordination Committee, and capacity building in the Pacific – a region marred by challenging terrain. Read here.



CCB Strategic Document

This document aims to set out the objectives and ambitions for the further development of the GFCE for 2023-2024. Looking at the CCB landscape and unique value of the GFCE, it also summarizes the GFCE's activities and evolution in response to key developments and challenges that are driving up demand for collaboration and networking. The document emphasizes the critical coordination role that the GFCE plays in CCB and invites the Community to embark on this next phase together. Read here.

Mainstreaming Gender doc



Gender is a crosscutting issue with direct relevance to achieving international peace and security, and as such has become an increasingly important topic in the field of cybersecurity. Understanding how gender considerations impact on and are impacted by behaviour in cyberspace has become a major policy objective of states and non-state actors alike. The GFCE intends to explore how its platform and community can support mainstreaming of gender in CCB. This concept note aims to catalyze discussion within the GFCE Community on mainstreaming gender in CCB and provide the impetus for stakeholders to engage around implementing commitments. Read here.

Program and Speakers Overview

Wednesday 14 September 2022	Thursday 15 September 2022
Opening Ceremony **Chris Painter,** *President GFCE Foundation Board* **Maartje Peters,** *GFCE co-Chair, The Netherlands* **Shri Alkesh Kumar Sharma,** *GFCE co-Chair, India* **Rick Harris,** *GFCE Advisory Board co-Chair*	**Roundtable work session 1: Strengthening Collaboration in the GFCE Community** **David van Duren,** *Director GFCE Secretariat* **Marjo Baayen,** *Director GFCE Secretariat*
GFCE Community Showcase Hour **Sithuraj Ponraj,** *Cyber Security Agency Singapore* **Gerard Elfa García,** *Capgemini* **Komal Bazaz Smith,** *DAI* **Andraz Kastelic,** *UNIDIR* **John Reyels,** *Germany* **Danielle Santos,** *NICE* **Jean-Louis Perrier,** *ACRC* **Timo Koster**, *Quad9*	**The GFCE's Regional Efforts** **Tereza Horejsova,** *GFCE Secretariat* **Sithuraj Ponraj,** *CSA Singapore* **Martin Koyabe,** *GFCE Africa Program Team* **Saia Vaipuna,** *GFCE Pacific Hub* **Valentina Name,** *Organization of American States* **Alexandra Adina Asgari,** *GFCE Secretariat*
Keynote on Cyber Capacity Building **Dr. Towela Nyirenda-Jere,** *AUDA-NEPAD*	**Western Balkans Breakout** **Vladimir Radunovic,** *DiploFoundation* **Silja-Madli Ossip,** *EU CyberNet* **Ilija Zhupanoski,** *North Macedonia* **Bruce McConnell,** *ORF America* **Artan Dreshaj,** *Kosovo** **Wouter Veenstra,** *GFCE Secretariat* **This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.*
GFCE Updates and Developments **David van Duren,** *Director GFCE Secretariat*	**Africa Breakout** **Martin Koyabe,** *GFCE Africa Program team* **David van Duren,** *GFCE Secretariat* **Enrico Calandro,** *Cyber4Dev* **Jaqueline Pateguana,** *GFCE Secretariat* **Velimir Radicevic,** *GFCE Secretariat*
Private sector perspective: What States should know on technical developments and their impact on CCB efforts **Eben Louw,** *IBM* **Olivia Blackmon,** *DAI* **Tim Appleby,** *Mandiant* **Nikolas Ott,** *Microsoft*	**APAC Breakout** **Saia Vaipuna,** *GFCE Pacific Hub* **Cherie Lagakali,** *GFCE Pacific Hub* **Steven Matainaho,** *Papua New Guinea* **Klee Aiken,** *FIRST* **Malisone Phommavichith,** *Lao PDR*
Panel discussion on the Global Conference on Cyber Capacity Building: Strengthening Cyber Resilience for Development **Francesca Spidalieri,** *GC3B Program Team* **Chris Painter,** *President GFCE Foundation Board* **Stephane Duguin,** *CyberPeace Institute* **Tal Goldstein,** *World Economic Forum* **Anat Lewin,** *World Bank*	**LAC Breakout** **Tereza Horejsova,** *GFCE Secretariat* **Valentina Name,** *Organization of American States* **Pablo Castro Hermosilla,** *Chile* **Cesar Moline,** *LAC4* **Robert Collett,** *Cybil Portal Team*
Ensuring Gender Sensitive Approaches and Inclusivity in Cyber Capacity Building **Louise-Marie Hurel,** *GFCE Advisory Board / Igarapé Institute* **Craig Gillies,** *Australia DFAT* **Cherie Lagakali,** *GFCE Pacific Hub* **Dr. Towela Nyirena-Jere,** *AUDA-NEPAD*	**Roundtable Work Session 2: Global Conference on Cyber Capacity Building** **Daniel McMurray,** *Conference Lead*
Confidence Building Measures (CBMs) Implementations and Capacity Building **John Reyels,** *Germany* **Szilvia Toth,** *Organization for Security and Co-operation in Europe* **Daniela Ruiz Dominguez,** *Mexico* **Arthur David,** *Global Affairs Canada* **Craig Gillies,** *Australia DFAT* **Sithuraj Ponraj,** *Cyber Security Agency Singapore*	**Opening Ceremony** **Chris Painter,** *President GFCE Foundation Board*