GFCE

GLOBAL FORUM ON CYBER EXPERTISE

ANNUAL REPORT

2022

CONTENTS

1

INTRODUCTION

The GFCE is a pragmatic, action-oriented and flexible platform for international collaboration in cyber capacity building (CCB). Read more on the GFCE's vision and check the highlights of 2022.

FOREWORD

In the past few years cyberspace continued to develop and becomes more complex, and the role of capacity building as a solution to these problems grows even more crucial. Over the course of seven years from the GFCE's establishment, the GFCE Community has maintained a flexible and diverse ecosystem geared towards the needs of its Members and Partners and that mobilizes multistakeholder engagement by design.

In 2022, we welcomed our Community to The Hague for the GFCE Annual Meeting 2022, the first in-person event after the COVID-19 pandemic. From the number of representatives attending - both old and new stakeholders - and their ongoing engagement with the GFCE's activities, we have seen that cyber capacity building is a powerful and necessary tool for change in the era of digital transformation.

Being able to bring together the Community to network, share experiences and most importantly to learn from each other, has been the cornerstone of our success over the past years. We are proud to see that last year, multiple achievements brought the GFCE's work forward:

- Engagement of the GFCE Community at in-person global and regional GFCE events;
- Strengthening the GFCE's regional presence with the establishment of liaisons and hubs;
- Facilitating the GFCE's engagement with the UN Processes;
- Increasing the match-making efforts through the Clearing House mechanism;
- Encouraging further cooperation around strengthening cyber resilience for development.

Building on the successes of 2022 and moving towards 2023, the GFCE is 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 reinforcing a demand-driven approach through expansion with regional (locally based) liaisons and offices. Thus, I am looking forward to continuing this journey, to maintain existing and developing new partnerships and consolidating together our commitment to strengthening cyber capacity building globally.

Thank you for your continuous support to the GFCE.

Chris Painter
President of the GFCE Foundation Board

2022 AT A GLANCE

3
YEARS SINCE THE ESTABLISHMENT OF THE GFCE FOUNDATION

6
GLOBAL & REGIONAL EVENTS

2
REGIONAL HUBS ESTABLISHED

+600
COMMUNITY PARTICIPANTS

+100 000
PEOPLE REACHED ONLINE

183
TOTAL MEMBERS AND PARTNERS

28
NEW MEMBERS AND PARTNERS

2
CLEARING HOUSE CASES FINALISED

4
RESEARCH PROJECTS FINALISED

+4 000
MONTHLY USERS ON THE CYBIL KNOWLEDGE PORTAL

2

COMMUNITY ENGAGEMENT

At the heart of the GFCE is the global multistakeholder community. As the GFCE aims to strengthen coordination, collaboration and avoid duplication of efforts, the GFCE Secretariat facilitates engagement to ensure the needs of the GFCE Community are being met. Community engagement occurs through regular global and regional events and through a continuous dialogue with our members and partners.

ENHANCING THE GFCE ECOSYSTEM

In 2022, some GFCE structures and roles underwent changes with new people from the wider cyber community joining the GFCE ecosystem.

New GFCE co-Chair on behalf of India

During the GFCE Annual Meeting 2022, Shri Alkesh Kumar Sharma was presented as the new GFCE co-Chair on behalf of India. On behalf of the Netherlands, the GFCE co-Chair is Ms. Maartje Peters. The co-Chairs, in collaboration with the Secretariat, advise on the planning of the GFCE annual and high-level meetings and report annually on the GFCE's activities and accomplishments. The GFCE co-Chairship of the Netherlands and India is evidence of the remarkable relationships that have become established under the GFCE umbrella.

New Advisory Board 2022-2024

The GFCE Advisory Board was established to further promote the role of civil society, academia and the technical community in CCB and the GFCE. The main role of the Advisory Board is to provide advice and support to the GFCE community and Foundation in decisions on the GFCE's functioning, activities and overall strategic direction. The new Advisory Board Members 2022-2024, which were announced during the GFCE Annual Meeting 2022, are: Richard Harris (MITRE), Louise-Marie Hurel (Royal United Services Institute), Ephraim Percy Kenyanito (ARTICLE19), Stephane Duguin (CyberPeace Institute), Elizabeth Vish (Institute for Security and Technology), Joe Burton (University of St Andrews), Nompilo Simanje (Media Institute of Southern Africa), Mateo Lucchetti (CYBER 4.0), Letitia Masaea (Pacific Islands Forum Fisheries Agency), Sorene Assefa (United Nations Economic Commission for Africa), Kevon Swift (Latin America and Carribbean Internet Addresses Registry).

GFCE-Pacific Hub Team

In 2022, the GFCE Pacific Team was established with Siosaia Vaipuna as the GFCE Pacific Hub Director and Cherie Lagakali as the Senior Advisor for Cyber Policy & Communications. The Pacific Hub team is responsible for leading the establishment of the Hub and to facilitate and coordinate the cyber capacity building needs and interests of the Pacific community.

New Working Groups Chairs

Working Group B on Incident Management & Infrastructure Protection was appointed a new Chair, Klée Aiken (Forum of Incident Response and Security Teams). Working Group A Task Force Strategy & Assessments was also appointed a new co-lead: Daniela Schnidrig (Global Partners Digital). Working Group D on Cyber Security Culture & Skills' new Chair was announced to be Steven Matainaho (Department of Information and Communications Technology, Papua New Guinea).

New Research Committee Members

The Research Committee supports the development and delivery of the annual Global Cyber Capacity Building Research, by helping to translate ideas into research questions. Last year, new members joined the committee: Tatiana Tropina (Leiden University), Nnenna Ifeanyi-Ajufo (Buckinghamshire New University) and Lilian Georgieva-Weiche (Deutsche Gesellschaft für Internationale Zusammenarbeit).

ACCOUNT MANAGEMENT

The GFCE's account management continues to connect with GFCE Members and Partners on a regular basis to ensure the GFCE meets the community's needs and adds value to their organization's work. In 2022, our account management efforts were demonstrated in:

- Global and regional GFCE meetings;
- Regular calls and meetings with individual Members and Partners;
- Multiple online GFCE webinars and meetings;
- Participation of the GFCE Secretariat in external events.

The GFCE has a truly multi-stakeholder community, comprising of governments, international organizations, non-governmental organizations (NGOs), private sector, think tanks, research organizations, technical associations and regional organizations, as illustrated in the graph below.

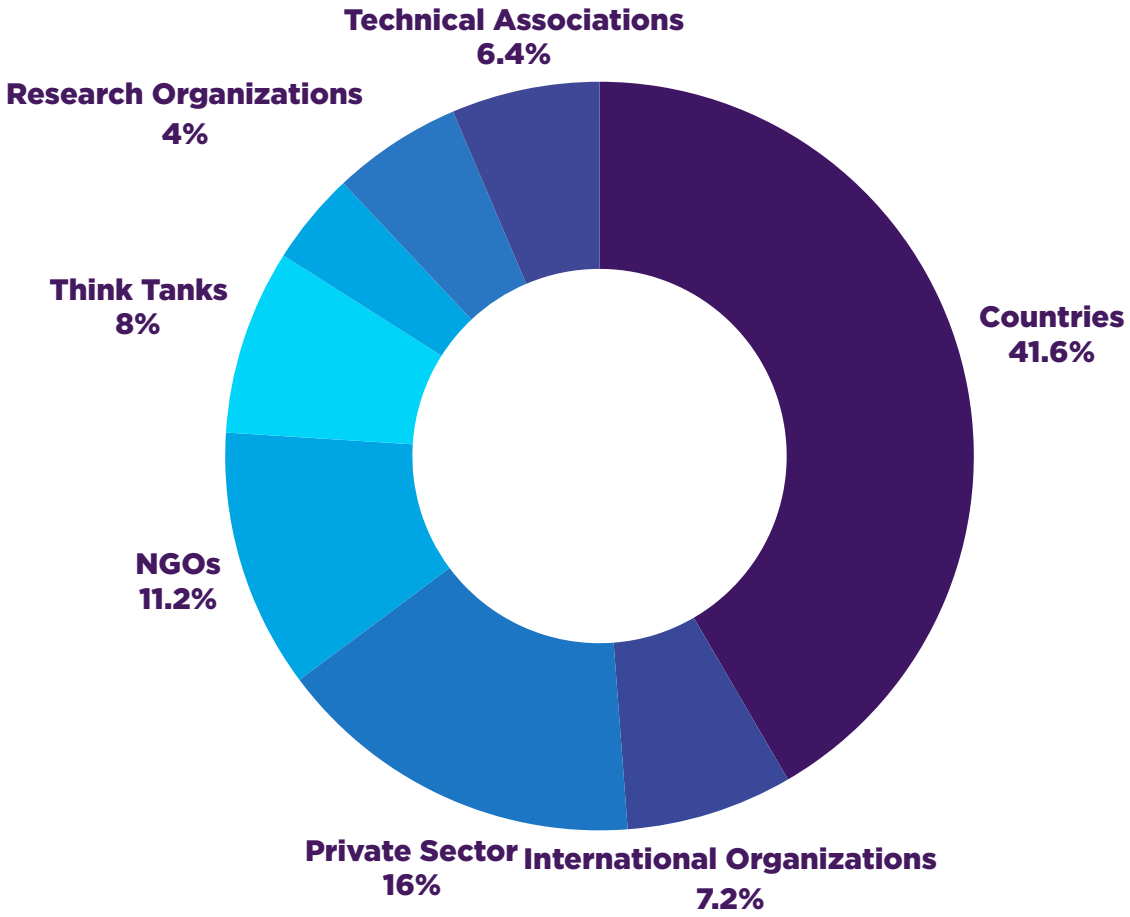


FIG. 1 A MULTISTAKEHOLDER COMMUNITY

COMMUNITY GROWTH

Together with a strong focus on developing the regional hubs, the GFCE community continued to grow with new members and partners from all corners of the world. The GFCE has continued to foster an environment in which the participation of all stakeholders continues to thrive and develop. As demonstrated in the figure below the GFCE Community has grown 16% in 2022, making a total of 183 Members and Partners.

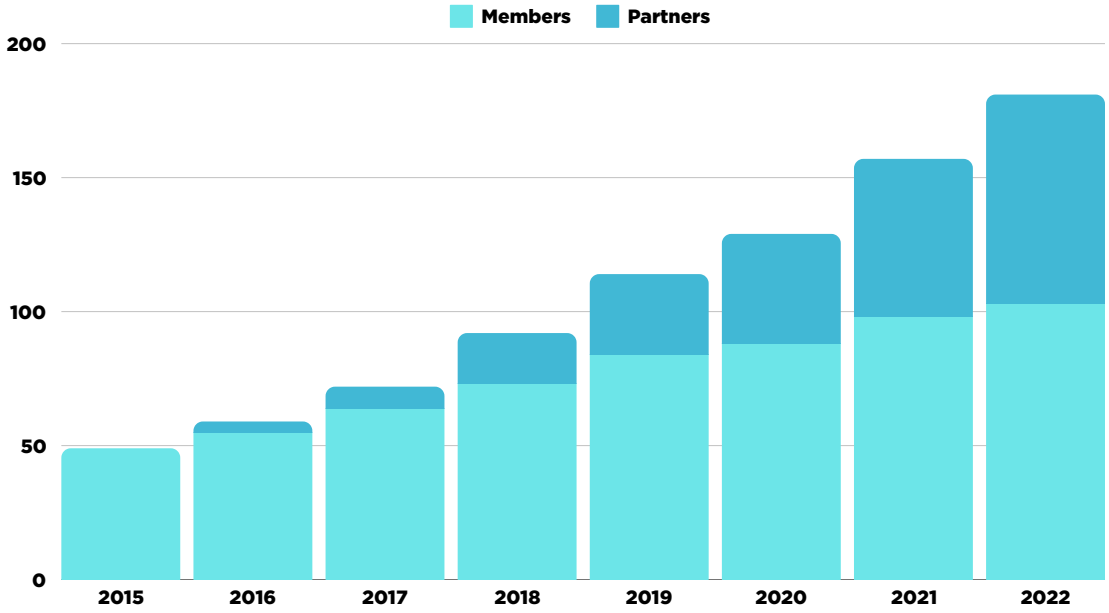


FIG 2. GFCE COMMUNITY GROWTH 2015-2022

In 2022, the GFCE welcomed 28 new stakeholders: 9 Members and 19 Partners.

NEW MEMBERS

- Republic of Congo
- Cameroon
- Standard Chartered Bank
- BAE Systems
- Mozambique
- Bhutan
- North Macedonia
- ABSA Bank
- Curaçao

NEW PARTNERS

- EU CyberNet
- Institute of Cyber Security for Society (iCSS)
- CyberLite
- CyberSafe Foundation
- United Nations Economic Commission for Africa (UNECA)
- Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)
- Center for Cybersecurity Policy and Law
- Quad9
- LAC4
- Stiftung Neue Verantwortung (SNV)
- European Institute for Political Studies in Moldova (EIPSM)
- Royal United Services Institute (RUSI)
- Institute for Security and Technology (IST)
- German Council on Foreign Relations (DGAP)
- Internet Society (ISOC)
- Cyber Academy
- Blavatnik ICRC (Interdisciplinary Cyber Research Center)
- Tony Blair Institute
- Global Anti Scam Alliance (GASA)

EVENTS

1
Global Event

5
Regional Events

+2 000
Participants

8
Community Projects Showcases

49%
Women Participants

+170
Multi-Stakeholders Present

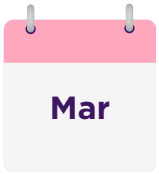
4
Continents Hosting GFCE Events

FIG 3. GFCE EVENTS STATISTICS 2022

EVENTS

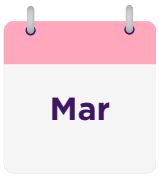
The GFCE hosts regular events to bring the community together to discuss current developments in CCB, receive updates on GFCE developments and further facilitate the strengthening of CCB through connecting resources and expertise globally. In 2022, the GFCE hosted both in-person and online meetings, with different stakeholders attending and actively participating in the events.

African Union-GFCE Collaboration Project, Accra



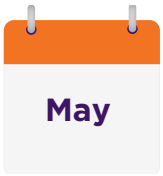
The first African Cyber Experts (ACE) Community meeting of 2022 was held in Accra. Topics such as as boosting cyber diplomacy, combatting cybercrime, awareness raising and enhancing gender equality were discussed. The Accra meeting in particular was important as it saw the official launch of the series of nine Knowledge Modules, which will be presented to the GFCE Community in early 2023. Read more here.

1st ECOWAS Workshop on Advancing Cyber Security, Accra



The workshop, sponsored by the German Federal Foreign Office and held in March 2022 in Accra, Ghana, was the first of two exploratory workshops aimed at capturing cyber capacity building priorities by the Economic Community of West African States (ECOWAS) member state representatives and the ECOWAS Commission, and creating a tailored program to address these needs. Discussions were held on necessary interventions in the area of boosting the cyber diplomacy footprint of ECOWAS member States in UN fora, as well as how best to approach the protection of critical infrastructure and services.

2nd ECOWAS Workshop on Advancing Cyber Security, Bonn



The second workshop aimed at measuring cyber capacity building needs was held in May 2022 in Bonn, Germany. It sought to hold interactive discussions on two more priority areas – measures to promote cybercrime combatting capabilities and the protection of vulnerable communities online, as well as data sovereignty and data protection. Based on the resulting recommendations from the two workshops, the ECOWAS Commission, German Federal Foreign Office and the GFCE produced the draft ECOWAS Action Plan for Advancing Cyber Security, which outlines the concrete deliverables that can be realized with ECOWAS Member States to measurably improve the level of cyber capacities in the four discussed areas. The Action Plan is to serve as a document to also rally resources and support for their implementation.

EVENTS

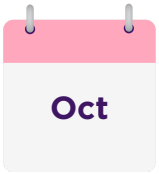
GFCE Annual Meeting 2022, The Hague

The GFCE Annual Meeting 2022, "Coordination for the Future", took place in the Hague and brought the GFCE Community together in person for the first time in almost three years. During the meeting, the Community reflected on the GFCE's developments and activities, explored the GFCE's coordination role in identified areas (e.g. gender inclusivity, UN processes, regional efforts), and exchanged ideas on key cyber topics. Read the report here.

African Union-GFCE African Cyber Experts Meeting, Online

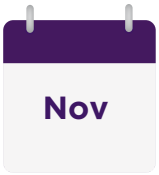
The GFCE organized the second ACE Community meeting virtually in September 2022. During the meeting, feedback was collected on the progress of the AU-GFCE Collaboration Project, and the study on 'Advancing Cyber Security with Africa', conducted by KPMG, was presented. The report's results, which will be available online in early 2023, show that most AU member states are progressing incrementally in enhancing their cyber capacities in terms of awareness and skills and legislation frameworks at a national level. Read more here.

GFCE South-East Asia Regional Meeting, Singapore



The GFCE Southeast Asia Regional Meeting took place in Singapore in October 2022, in cooperation with the Cybersecurity Agency of Singapore (CSA), during the Singapore International Cyber Week (SICW). The meeting brought together the GFCE community and ASEAN stakeholders to identify opportunities and challenges for CCB in the region and share good practices and knowledge.

GFCE Latin America and Caribbean Meeting, Santo Domingo



The GFCE Secretariat, together with the Secretariat of the Inter-American Committee Against Terrorist (CICTE) of the Organization of the American States (OAS) and the Latin American and Caribbean Cyber Competence Center (LAC4EU) organised the GFCE Regional Meeting in the Americas in November 2022 in the Dominican Republic. The meeting served as an opportunity to introduce the progress of the GFCE Hub for the Americas and the priorities for the future, introducing ways for involvement to key regional actors. Read the report here.

EVENTS

GFCE Africa Regional Meeting, Addis Ababa

Nov

The GFCE Africa Regional Meeting took place in Addis Ababa in November 2022. Some topics covered were the medium to long-term goals to be included in the Africa Agenda on Cyber Capacity Building (AA-CCB), as well the results of the African Union-GFCE Collaboration Project, supported by the Bill and Melinda Gates Foundation.

GFCE Global CCB Research Agenda Session at the Global Constellation of Capacity Centres Annual Conference, Cape Town

Nov

The Research Agenda 2022-2023 was presented at the Global Constellation of Capacity Centres Annual Conference that took place in Cape Town in early November 2022. During the presentation, members of the GFCE Research Committee, the GFCE Secretariat and researchers that have collaborated on the Research Agenda had the opportunity to introduce the Research Agenda, discussing the results achieved so far and their relevance for African stakeholders whilst interacting with the audience in order to explore potential ways of strengthening the Research Agenda's impact, ownership, dissemination and areas of improvement vis-à-vis the African Academic Community. The GFCE's Research Committee has continued to meet regularly to reflect on the research agenda process, suggest improvements and explore avenues to strengthen cooperation with the academic community. Read more here.

Study Visit for ECOWAS Members States Representatives, Brussels

Dec

As part of the recommendations set out in the ECOWAS Action Plan for Advancing Cyber Security, in December 2022, the German Federal Foreign Office, the GFCE and EU Cyber Direct facilitated a Study Visit for ECOWAS cyber experts to Brussels, Belgium. The aim of the visit was to share best practices from Directorates General, the European External Action Service, as well as on cyber effort coordination mechanisms in the EU. Further, it aimed to promote discussion about inter-regional cooperation in cyberspace between the EU and ECOWAS, and explore further implementation modalities for the Action Plan recommendations in 2023 and beyond.

COMMUNICATIONS AND BRANDING

In 2022, the GFCE Secretariat continued implementing its external communication activities focusing on providing accurate updates to the GFCE Community, increasing GFCE brand awareness and fostering community engagement. Moreover, the Secretariat further strengthened its communication channels and tactics and ensured that all requests from the GFCE Members and Partners were responded quickly.

Throughout the year, the GFCE's social media accounts generated over 730 000 impressions and more than 4 000 interactions from 171 social media posts, covering topics such as GFCE developments, events, Members and Partners updates and other important CCB milestones. The Secretariat focused on maintaining a strong digital presence, and developing numerous pieces of visual communication (infographics, web visuals, videos, illustrations and other type of interactive content).

In addition to a strong online presence, the GFCE brand was showcased in 12 in-person events across Europe, North America, South America, Africa and Asia. This included the use of promotional banners, informational booklets, and GFCE-branded memorabilia such as sustainable reusable coffee cups, luggage tags, USB flash drives, and tote bags. Strong emphasis was placed on the sustainability of branded materials, as participants of GFCE events were provided the opportunity to select their own GFCE items at GFCE Goodie Stations to take home.

Overall, 2022 saw the GFCE brand strengthen its image and reach globally, reflecting the growth that the GFCE Community has had over 2022.

FIG. 4 SOCIAL MEDIA AND WEBSITE REACH IN 2022

GLOBAL CYBER EXPERTISE MAGAZINE

FIG 5. ISSUE 11 OF THE MAGAZINE

The Global Cyber Expertise Magazine is a joint initiative by the African Union, European Union, the Global Forum on Cyber Expertise and the Organization of American States. It aims to provide cyber policymakers and stakeholders insight on CCB projects, policies and developments globally.

Issue 11 was published in September 2022 at the GFCE Annual Meeting 2022. The cover story takes a look at how the Global Conference on Cyber Capacity Building (GC3B) is making 2023 the year of Cyber Resilience for Development. Also under the global developments section, we spotlighted why the resilience of NGOs in cyberspace should be a top priority and the role of the CyberPeace Builders in achieving this. Following this, we dove into how regional multistakeholder cyber capacity building is being advanced through the Global Cyber Policy Dialogues.

From the Americas, the need for cyber capacity building and the cybersecurity situation of the region was explored. We then discovered how the region is responding specifically to the shortage of cybersecurity professionals through education, training and capacity-building opportunities.

From Europe, the UK's Digital Access Programme was highlighted, exploring how it offers a holistic approach to building and sustaining cyber capacity. Additionally, an article uncovered strategies for cyber diplomacy capacity building.

From Africa, the developments of the Africa Cyber Capacity Building Committee were described, in addition to how African students' strategic thinking on cybersecurity is being developed through cyber policy competitions such as the Cyber 9/12 Strategy Challenge.

From Asia and Pacific, we featured an article reflecting on some cyber incidents that affected the Pacific in the past year, and how these inform the role of the GFCE in supporting the Pacific's cyber capacity building efforts.

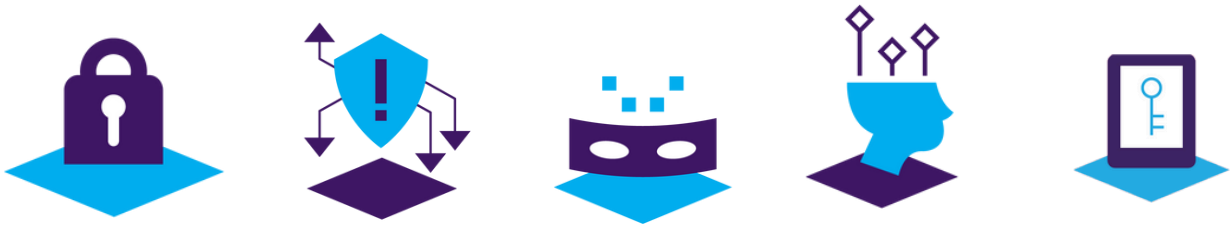
3

WORKING GROUPS & TOOLBOX

The GFCE Working Groups together with the GFCE Toolbox - comprised of the Cybil Knowledge Portal, the Global CCB Research Agenda and the Clearing House - support the practical implementation of the GFCE's CCB efforts.

WORKING GROUPS

The GFCE Working Groups were established in 2018, following the GFCE Community's endorsement of the Delhi Communiqué on a Global Agenda for Cyber Capacity Building. Based on the thematic priorities identified in the Delhi Communiqué, the Working Groups are organized into the following five themes:



A. Cyber Security Policy and Strategy

B. Cyber Incident Management and Critical Infrastructure Protection

C. Cybercrime

D. Cyber Security Culture and Skills

E. Cyber Security Standards

The Working Groups provide a communal space for GFCE Members and Partners to discuss thematic CCB issues, share knowledge and updates with each other, exchange best practices, and deconflict CCB efforts. They play a strong role in keeping the community connected and bringing new stakeholders into the GFCE. Some key achievements of the Working Groups in 2022 are presented below:

Developed the interactive web-based tool "Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle"
Translated "Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle" into French and Spanish
Pubished the "Short Guide to Stakeholder Engagement on NCS Development"
Launched a new online series on the "UN Cyber Processes (GGE, OEWG, AHC)" to delve deeper into the processes from a CCB lens
Continued the multi-part "Cybercrime Series", with one session on the role of CCB combatting ransomware and one on addressing the use of cryptocurrencies for criminal purposes

Published the "CIM Cybil Portal Resources Guide"
Published an updated "Global CSIRT Maturity Framework (GCMF)"
Published a report on "Developing Cyber Security as a Profession"
Initiated consultations with the private sector and technical community to raise awareness and promote capacity building on open Internet Standards regionally through the "GFCE Triple-I initiative"

CYBIL KNOWLEDGE PORTAL

The Cybil Portal (CybilPortal.org) is a knowledge sharing platform for the international CCB community. It is a place where governments, funders and implementing agencies can find and share best practices and practical information to support the design and delivery of CCB projects and activities.

Following the launch of Cybil 2.0 in December 2021, which addressed feedback and suggestions for improvement by the GFCE Community, the Cybil Portal Team has offered personalized support to governments and organizations with updating their capacity building project information on the Portal. The new project page template strives to offer more complete and user-friendly access to project information to improve the quality of content. Moreover, the second half of 2022 has seen Cybil strengthen its collaboration with other cyber databases and portals, such as UNIDIR's Cyber Policy Portal and EU CyberNet's CCB Project Mapping Database. Towards 2023, the Portal Team will continue to explore ways of enhancing collaboration with other cyber portals to continue to avoid duplication and promote coordination of efforts.

Cybil

www.cybilportal.org

Cybil statistics in 2022:

+4000
Visitors

Over 2022, the Cybil Portal received more than 4,000 unique visitors on average every month.

+100,000
Page Views

Cybil had a total of over 100,000 site unique visits from more than 180 countries worldwide.

135
Tools & Publications

Around 135 tools & publications were uploaded to the Portal over the last year, including guides, academic papers, reports and studies amongst other CCB related content.

40
New Projects

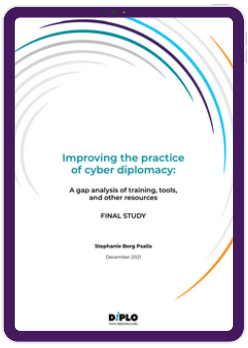
The Cybil Portal Team added more than 40 project pages with the new template, enhancing content quality and ensuring user-friendly information.

80+
Events

Over 80 CCB related events were uploaded to Cybil over the past year, such as international cyber conferences, webinars and regional events.

GLOBAL CCB RESEARCH AGENDA

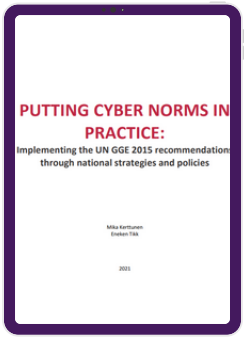
The Global CCB Research Agenda is a tool developed by and for the GFCE Community to provide research and analysis for the wider cyber community. Four research projects that were commissioned through the GFCE Global CCB Research Agenda 2021 were published in early 2022 on the Cybil Portal. To present the findings and raise awareness on the reports, the GFCE launched a four-part Research Webinar Series in 2022, involving discussions between research teams and experts in a panel setting. The recordings of the webinars and the research reports are available on Cybil:



Improving the practice of cyber diplomacy: Training, tools, and other resources

Watch Webinar | Read Report

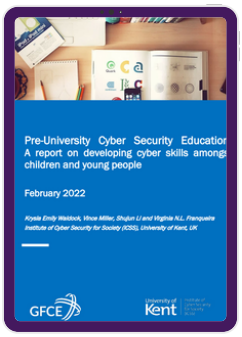
This study analyzes aspects of capacity development to increase the engagement of every country, that is, the availability of training opportunities, tools, and other resources and their reach and level of adoption. The survey conducted as part of this study confirmed that training and tools are indeed available, but they are not reaching everyone. The findings also uncovered the reasons why practitioners are often not taking any, or further, training and why they were not making use of the whole range of tools available to help them in their cyber diplomacy work.



Putting Cyber Norms in Practice: Implementing the UN GGE 2015 recommendations through national strategies and policies

Watch Webinar | Read Report

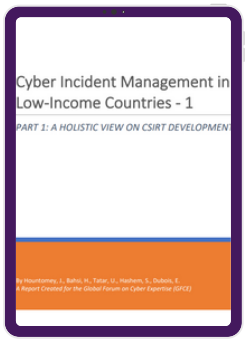
Because each country has its own starting point, goal and trajectory for implementing the UN's GGE 2015 recommendations, this Implementation Guide introduces various approaches that can be, and have been, adopted to implement norms of responsible state behaviour. The Implementation Guide seeks to facilitate, inform and promote collaborative and coordinated efforts to maintain and further develop an open, free, peaceful and stable cyberspace through adequate national, regional and global cybersecurity practices.



Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people

Watch Webinar | Read Report

This report provides results from a research project about cyber security education and skills development for children and young people (up to the age of 18) in a pre-university setting. The results learned from the research led to a number of key findings and main recommendations, which we hope can help stakeholders around the globe, to improve cyber security education in a pre-university setting.



Cyber Incident Management in Low-Income Countries

Watch Webinar | Read Report

This report discusses the findings and recommendations of the "Cyber Incident Management in Low-Income Countries" project which aims to create a tailorable guide for low-income countries to develop or improve their CSIRT capabilities in an affordable way to respond to the evolving cyber threat environment effectively.

CLEARING HOUSE

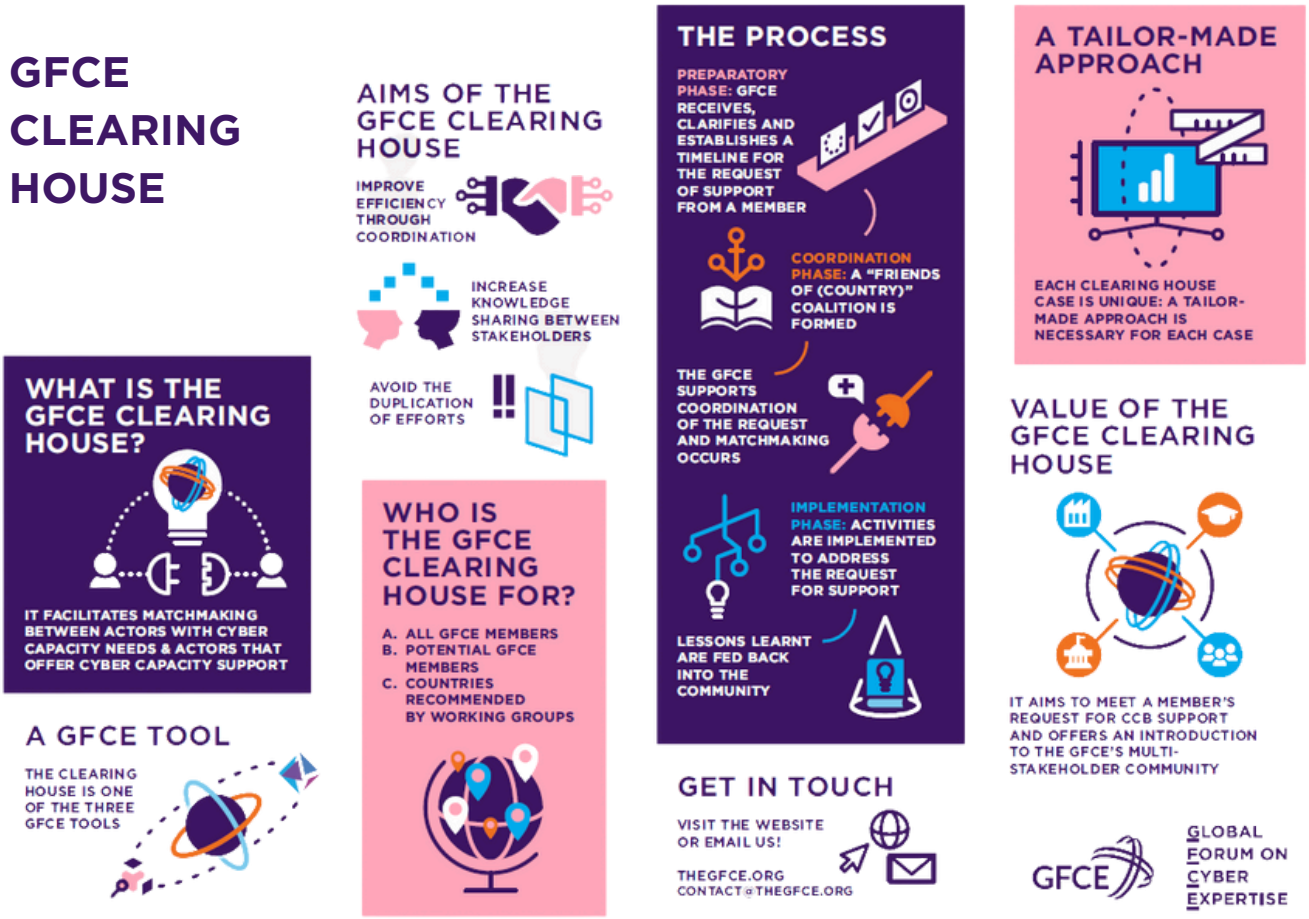


FIG. 6 GFCE CLEARING HOUSE MECHANISM

At the establishment of the GFCE in 2015, the Clearing House function was created to facilitate matchmaking between GFCE Members who have cyber capacity needs with GFCE Members and Partners who can offer cyber capacity support in the form of expertise and/or resources.

In 2022, the GFCE's focus was to scale-up capacity to support countries in defining their cyber capacity needs and matching them with existing expertise from the community. To achieve this, a three-pronged approach was used: (1) a baseline analysis of CCB gaps and priorities in 35 African nations was conducted through the AU-GFCE project, (2) the GFCE Secretariat appointed a new Clearing House Coordinator to lead the coordination efforts of meeting the demands from selected countries; and (3) the Clearing House Coordinator engaged with the GFCE Regional Hubs to support demand-driven sub-regional level projects. As a result, the Secretariat received requests for support from two member countries, the Republic of Congo and Sierra Leone, the latter of which received offers of support from several GFCE Community members, including the ITU and the World Bank's Cybersecurity Multi-Donor Trust Fund.

4

INTERNATIONAL COLLABORATION

To strengthen cyber capacities and expertise, the GFCE focuses on facilitating international and regional collaboration by coordinating implementation efforts, identifying CCB needs and avoiding the duplication of efforts.

AFRICAN UNION-GFCE COLLABORATION PROJECT

Through the backing of the Bill and Melinda Gates Foundation, in 2021, the AU and GFCE took steps towards establishing a sustainable, demand and community-driven ecosystem for CCB in Africa. In July, a comprehensive mapping exercise and gap analysis was shared with African stakeholders that sought to identify and categorize needs within the themes of tthe GFCE's Working Groups. Based on this analysis, work has begun on creating a series of Knowledge Modules aiming to provide African stakeholders with a collection of resources and accumulated experiences and best practices from the GFCE and African CCB communities. The project's dedicated team reached out to all 54 AU countries, with more than 20 having either engaged with the GFCE to share their CCB needs, or have nominated members to the newly established community of African Cyber Experts (ACE). These experts came together for the first time in November 2021 in the Hague, to enhance ties with one another, share knowledge and best practices, as well as input on the evolving Knowledge Modules.

The community and resources brought together under the AU-GFCE project are helping establish a more permanent African-owned and operated GFCE Hub on the continent, which will serve to coordinate CCB efforts, reduce duplication and match local needs with global supply. As part of the emerging Hub, the African CCB Coordination Committee was formed, consisting of over 25 associations, Regional Economic Communities and private sector entities. These developments, taken together, will provide GFCE with the tools necessary to offer both the donor and beneficiary communities an African CCB Agenda to unlock further resources and funding and address long-standing needs in 2023.

WOMEN IN INTERNATIONAL SECURITY AND CYBERSPACE FELLOWSHIP

The Women in International Security and Cyberspace Fellowship (WIC) aims to ensure equal representation of women in the United Nations cyber negotiations. The program seeks to develop cyber governance capacities, providing access to workshops, training, and travel support to fellows' participation in UN First and Third Committee processes.

The fellowship is jointly organized and sponsored by the Governments of Australia, Canada, the Netherlands, New Zealand, the United Kingdom and the United States. In 2022, services provided by the GFCE Secretariat supported the participation of 39 fellows from 26 countries. The majority of the fellows (31) have actively engaged in the UN First Committee, with the remainder (8) participating in the UN Third Committee. Across 2022 there have been two substantive sessions of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), and three substantive sessions of the Ad-Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC).

The fellows also participated in three training opportunities. In January 2022, the UK organized a workshop on cybercrime, which was delivered by Chatham House to those fellows following the AHC process. A second workshop was organized in May 2022 as a follow-on from the initial primer, looking more closely at the AHC process and the role that gender plays in the convention. In July 2022, fellows attending the 3rd substantive session of the OEWG participated in a week-long training organized by Australia and delivered by the United Nations Institute for Training and Research (UNITAR).

TRIPLE-I INITIATIVE

The GFCE Triple-I initiative is meant to facilitate awareness raising and capacity building events in different regions of the world in order to enhance justified trust in the use of Internet and/or email in those regions (specific priorities to be determined by stakeholders in the region). The Triple-I supports awareness raising on a number of state-of-the-art open internet security standards and instigates take up of internet standards by building on good practice experiences.

In September 2022, the GFCE and inSIG hosted the Triple-I Workshop in India, during which participants including global and regional experts, regional Internet stakeholder groups, governments, businesses and technical community, contributed to finding solutions to strengthen an open end-to-end Internet. The event focused on three pillars: better use of today's open internet standards, inspiration from good practice actions and planning for a more trusted internet, marketplace for action. Following the meeting, a group of volunteers announced their willingness to step up and come with a proposed way forward for actioning these proposals: enhancing justified trust, as a key multistakeholder supported step to support the Indian government is one of the aspirations with regards to Digital India. With this, the workshop achieved its highest aspiration – support local stakeholders to define and commit to local action, making best use of global experience and resources. Read more about the Triple-I Initiative on the GFCE website.

GFCE WOMEN IN CYBER CAPACITY BUILDING

Launched in 2020, the GFCE Women in Cyber Capacity Building (WiCCB) Network brings together female cybersecurity professionals to connect and raise awareness on capacity building issues, encouraging the inclusion and empowerment of women in the field. In 2022, the Secretariat initiated a series of online events on topics related to cyber and advancing the objectives of the network, with the first event related to women's participation in the high-level negotiations of the OEWG (Open-Ended Working Group) on security of and in the use of information and communications technologies. A follow up in-person was held in The Hague during the GFCE Annual Meeting 2022, during which members of the Network had the opportunity to network and discuss new ideas and activities for the group to develop in 2023. The Secretariat further connected with other networks and initiatives for women in cyber security, looking into opportunities to join forces to further address the gender cyber workforce gap. In 2023, the GFCE aims to form a basis for discussion on mainstreaming gender in cyber capacity building in order to produce a set of recommendations for action that the GFCE can take forward in promoting gender equality, diversity and social inclusion considerations in CCB. During these discussions, the WiCCB Network will play an active role in ensuring the integration of gender equality across the GFCE ecosystem.

5

REGIONAL COLLABORATION

To strengthen cyber capacities and expertise, the GFCE has moved towards a demand-driven approach, strengthening its regional presence and coordinating implementation efforts and identifying regional CCB needs through the GFCE Regional Hubs and Liaisons.

GFCE HUB FOR THE AMERICAS

Hosted at the headquarters of the Organization of American States in Washington, DC, the Americas and the Caribbean is a promising and active hub of the GFCE. Under the stewardship of the CICTE Secretariat, the GFCE Hub for the Americas has concentrated on mapping regional projects to feature at the Cybil Portal, planning of the regional capacity building agenda and worked closely with the GFCE Secretariat to ensure the regional efforts align with the GFCE's global efforts.

The GFCE Regional Meeting for the Americas was held in Santo Domingo, Dominican Republic in November 2022, in cooperation with the LAC4 Centre and served as an opportunity to introduce the GFCE to new potential members and partners and in particular, significant progress was made in relation to inputs for the regional capacity building agenda, which is a priority for 2023 and facilitated interaction with several other donors and implementers. The meeting besides others covered one of the priority issues identified in the region – cybersecurity workforce development, a topic also high on the agenda of the GFCE Working Group D. The GFCE Hub for the Americas will be focused on designing initiatives in the region for a more cohesive capacity building and identifying funding to ensure that engagement in the region is increased and strengthened.

GFCE-PACIFIC HUB

Commissioned in 2020 and finalized in November 2021, a proposal for the establishment of the GFCE Pacific Hub has been presented and adopted by a donor group that includes the United States, New Zealand, Australia and the United Kingdom. Mr Siosaia Vaipuna, based in Tonga, was appointed as the Hub Director, alongside the hire of Ms Cherie Lagakali, Senior Advisor for Cyber Policy and Communications, based in Fiji.

Through engagement activities, the hub continues to collect and share information with different stakeholders on current CCB initiatives in the region. During country visits, the hub has demonstrated its capability to bring together donors and implementers to respond to a need from the community. This was evident in the planning and then success of Cyber Smart Samoa and SamHack. At the fringes of global and regional events, the hub has been presented with several opportunities to hold side meetings with stakeholders from different donor and implementer communities to facilitate CCB efforts, as well as coordinate with representatives from Pacific Island countries about CCB in their community. The hub team has visited Tonga and Samoa, meeting high level officials including the Prime Minister and Attorney General of Tonga, the Minister for Information and Communication in Samoa as well as operational teams from government, non-government organizations and the private sector in both countries. The team has also participated in regional events like the Pacific Cyber Security Operational Network (PaCSON) AGM, Pacific Island Law Officer's Network (PILON) Cybercrime Workshop and on the global front, the team has been involved in the GFCE Annual Meeting and the 17th annual meeting of the Internet Governance Forum (IGF).

AFRICA

The GFCE's efforts to enhance, coordinate and prepare future CCB initiatives in Africa from the past three years have culminated in 2022. In the area of community building, the Africa Cyber Experts (ACE) Community and the CCB Coordination Committee have met regularly, becoming recognizable fora for the exchange of best practices, sharing capacity building needs, laying out strategic guidelines and promoting CCB tools. The Committee in particular has played an important role in framing the strategic framework within which CCB initiatives can be made more strategic, and are currently working on a CCB Agenda for Africa, set to be presented in 2023. These communities are well placed to provide key expertise, views and sustainability to any demand-driven CCB initiative in the region. However, demand-driven CCB efforts are only as effective as the capacity building needs in Africa are accurately captured, which is why the GFCE has commissioned KPMG to capture main CCB challenges, needs and recommendations in Africa.

Tailored and iterative capacity building tools were also in the spotlight, with the body of nine CCB Knowledge Modules for Africa, covering topics such as cyber diplomacy, critical infrastructure protection, cybersecurity culture, awareness, workforce & skills, standards & certification, and more. The Knowledge Modules have been shared with the ACE Community through a series of guided CCB Enhancement Webinars, and will be shared with the GFCE community in early 2023. Finally, the GFCE recognizes the unique developmental, security and societal contexts in each of the five African regions. This is why the GFCE was proud to have partnered with the German Federal Foreign Office and the ECOWAS Commission in 2022 to facilitate a series of workshops on discussing how to boost levels of cyber readiness and capacities in West Africa in areas of cyber diplomacy skills development, critical infrastructure protection, protection of vulnerable communities online and data sovereignty. The GFCE helped create the Action Plan on Advancing Cyber Security with ECOWAS for 2022 – 2025.

SOUTH EAST ASIA

The GFCE has a long term cooperation with Singapore (including having organised the 2018 Annual Meeting there) and has concrete plans to establish its physical Southeast Asia hub there, in close cooperation with the Cyber Security Agency of Singapore (CSA) and the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCEE).

The GFCE Southeast Asia regional meeting took place during the Singapore International Cyber Week (SICW) in October 2022 – focusing on the importance of CCB in the UN development agenda and collecting region-specific inputs on capacity needs. The creation of a GFCE SEA Liaison position, in partnership with CSA, was announced by Singapore's Senior Minister and Coordinating Minister for National Security, Mr. Teo Chee Hean, at the SICW Opening Ceremony. The appointment for this position is expected to take place in 2023. Specific efforts will be made to attract more members and partners from the region, including hosting some of them at the next GFCE Annual Meeting.

EUROPE

The GFCE supports coordination of efforts in Europe by acting as a neutral broker of information on projects, participants, tools and beneficiaries. A key aspect of this coordination is the Cybil Knowledge Portal which offers updated information regarding projects within Europe and projects funded or implemented by European actors abroad. An analysis of the CCB landscape in the region revealed three notable regions that would benefit from increased coordination: Western Balkans, Ukraine and Eastern Europe and Georgia & South Caucasus. Moreover, an analysis of the themes of ongoing projects revealed that European funded projects mainly focus on 'Strategy & Cyber Diplomacy' in terms on number of projects.

WESTERN BALKANS

Several members of the global community have called for more efficient coordination of cyber capacity building coordination in the Western Balkans. The GFCE has taken an active role in efforts to bring together key donors, implementors and recipient countries to explore some practical and concrete ways of more transparent coordination, that would avoid duplication of efforts and unfilled gaps in cyber capacity needs. Several meetings, including an in person gathering during the GFCE Annual Meeting in the Hague in September 2022, took place.

6

CORPORATE

In 2019, the GFCE Foundation was established to ensure that the GFCE can grow sustainably and become truly international, supporting the ongoing efforts of the GFCE Secretariat in facilitating the GFCE Community.

GFCE FOUNDATION

The GFCE Foundation provides an independent vehicle for the GFCE to continue to grow, internationalize and increase its impact through multiple donor funding. Under the wings of the Foundation, the GFCE Secretariat has an invaluable role in facilitating the GFCE network and its activities and will continue to do so even more effectively by expanding and internationalizing the team this year. In 2022, the Foundation brought the GFCE a step further towards strengthening cyber capacity and expertise globally through the establishment of the GFCE Regional Hubs, the organization of several in-person GFCE meetings and through the constant engagement of the GFCE Community in CCB initiatives and projects. In 2023, the Foundation Board will keep supporting and working together with the broader GFCE Community and the Secretariat to contribute to the steady growth that the GFCE has seen since its creation in 2015.

7

GFCE PRIORITIES 2023

Towards 2025, our mission is to ensure that the GFCE is the leading coordination platform for CCB stakeholders and activities on a global and regional level. To achieve this, the GFCE will focus the next two years to strengthen global cooperation, regional coordination, and local collaboration in CCB.

GLOBAL COOPERATION

Global Cooperation: Expand the GFCE network, focusing on inclusivity

The GFCE aims to cooperate globally with and connect CCB actors to strengthen connections and mature the GFCE ecosystem. An important milestone for the GFCE in the coming years is the Global Conference on Cyber Capacity Building (GC3B) which supports catalyzation of the GFCE's ambitions on global cooperation.

REGIONAL COORDINATION

Regional Coordination: Develop regional coordination to bridge the national and global level

It is essential to anchor CCB actors with our regional coordination presences to bridge the national and global level. The regional level allows the GFCE to take on a coordination role to ensure a demand-driven approach, prioritizing country's needs in cyber capacity building activities. The GFCE's regional hubs are the cornerstone for coordination through connecting with the regional CCB stakeholders, identifying needs, and sharing available expertise. Therefore, the GFCE has the following regional ambitions.

LOCAL COLLABORATION

Local collaboration: Empower local stakeholders by connecting to the GFCE ecosystem

The impact in cyber capacity building is most prominently made at the local level. With this in mind, it is important for local stakeholders to be connected to the GFCE ecosystem, which will lead to more effective identification and addressing of national CCB needs. Therefore, the following ambitions are set to support local stakeholder collaboration.

IDENTIFIED PRIORITIES

To achieve this, there are five main priorities identified below:

1.Foster inclusivity in the GFCE network: ensure an inclusive network that includes all relevant stakeholders active in CCB, including strong private sector and civil society participation and linking to the development community.

2.Empower the GFCE Regional Hubs in Africa, Latin America, Caribbean, Pacific and South-East Asia: to support needs analysis, regional coordination, and delivery of CCB activities. Each hub will:

- Build a regional multi-stakeholder CCB community.
- Identify and prioritize the needs for each region and country through developing demand-driven regional CCB agendas.
- Establish regional clearing house programs prioritizing south-south cooperation with (expertise) support from the GFCE community.

3.Establish a global CCB agenda: as an outcome of the GC3B process, steered by the GFCE community, to create a global agenda to support the facilitation of global and regional CCB priorities.

4.Scale up information sharing within the CCB ecosystem: by aiming to have all relevant projects and resources on Cybil to provide a good overview of who does what, where and when. Specifically, to make Cybil more inclusive with information from the Global South and encourage south-south cooperation success stories.

5.Spearhead and coordinate efforts to mainstream gender in CCB: support activities and analysis that encourage gender-sensitive CCB, as well as coordinate with and complement stakeholder efforts to mainstream gender in CCB.

Change is constant, and we need to continually adapt to ensure the GFCE remains the leading platform for matchmaking and coordinating the global CCB community. We will continue to embrace innovation, share knowledge, and build on each other's experiences and ideas. To make this possible, we need to work together and offer mutual support – across cultures, borders, and stakeholder groups. The GFCE Secretariat invites your insights, collaboration and ongoing support as we move forward together.

LIST OF ABBREVIATIONS

ACE	African Cyber Experts
AHC	Ad Hoc Committee
ASEAN	Association of Southeast Asian Nations
AU	African Union
CCB	Cyber Capacity Building
CICTE	Inter-American Committee against Terrorism
CIIP	Critical Information Infrastructure Protection
CSA	Cyber Security Agency
CSIRTs	Computer Security Incident Response Teams
ECOWAS	Economic Community of West African States
GC3B	Global Conference on Cyber Capacity Building
GCMF	Global CSIRT Maturity Framework
GGE	GGE
HSD	The Hague Security Delta
ICT	Information and Communications Technology
IGF	Internet Governance Forum
LAC	Latin America and the Caribbean
LAC4EU	Latin American and Caribbean Cyber Competence Center
NCS	National Cybersecurity Strategy
NGOs	Non-governmental organizations
OAS	Organisation of American States
OEWG	OEWG
PPP	Public-Private Partnership
SICW	Singapore International Cyber Week
UN	United Nations
UNITAR	United Nations Institute for Training and Research
WG	Working Group
WiC	Women in International Security and Cyberspace Fellowship
WiCCB	Women in Cyber Capacity Building

ACKNOWLEDGEMENTS

The GFCE Foundation Board and the GFCE Secretariat would like to thank the GFCE Community, including its Members and Partners, the committees and individuals on their personal capacity who contributed to the GFCE successes in 2022.

The GFCE Annual Report 2022 is distributed to GFCE Members and Partners and is available for download on the GFCE website.

Publication and Design: GFCE Secretariat

Copyright © 2023 GFCE Secretariat
All rights reserved. No part of this publication may be reproduced, stored or transmitted in any form, or by any means, photocopying, recording, otherwise, without prior consent of the publisher.

CONTACT

Wilhelmina van Pruisenweg 104, 7th floor
2595 AN The Hague, The Netherlands

+31 (0)70 204 5030

www.thegfce.org

contact@thegfce.org

@theGFCE