GFCE

Global Forum on Cyber Expertise

GFCE CONSULTATION MEETING 2021 | REPORT

Strengthening cyber capacity and expertise globally through international collaboration.

GFCE CONSULTATION MEETING 2021

The Global Forum on Cyber Expertise (GFCE) has evolved into a broad and diverse multi-stakeholder community of more than 130 members and partners. For six years this community works to achieve its mission of strengthening international collaboration on cyber capacity building and expertise on a global scale.

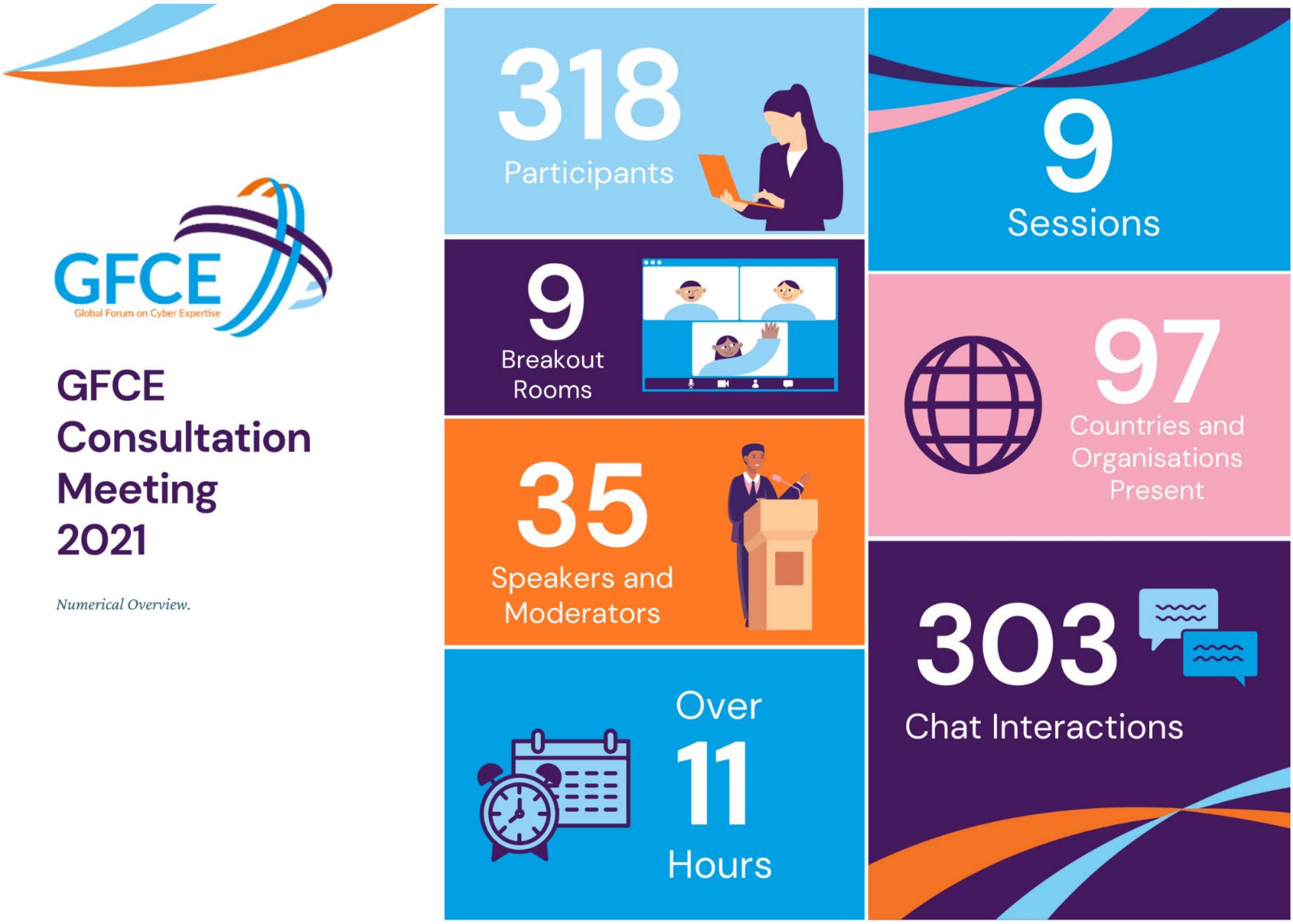
After the success of the GFCE virtual events and engagements across the past year, the GFCE hosted a virtual Consultation Meeting on 15-16 June 2021. Expanding on the Strategic Building Blocks presented to the community during the GFCE Annual Meeting 2020, the Consultation Meeting was centered around discussion on the achievements of the community thus far and laying out the priorities and milestones for the GFCE over the coming year.

The two-day Consultation Meeting provided a platform for GFCE Members and Partners not only to present updates on their projects and initiatives, but also represented a chance for the community to give its input on common objectives in the development of the GFCE ecosystem and engagements in the Pacific, Africa, Europe and Latin America and Caribbean regions.

CONTENTS:

ENGAGEMENT OVERVIEW

GLOBAL CYBER EXPERTISE MAGAZINE



GFCE Consultation Meeting 2021

Numerical Overview.

318 Participants

9 Sessions

9 Breakout Rooms

97 Countries and Organisations Present

35 Speakers and Moderators

303 Chat Interactions

Over 11 Hours

Opening & Strategic Way Forward	Day	Session	Participants
⇧Top	1	1	141

SESSION OBJECTIVES:
The aim of this session was to discuss the way forward for the Global Forum on Cyber Expertise. The GFCE Community were asked for their input on the proposed approach and to add their own suggestions as to what the priorities for the GFCE should be over the coming years.

KEY TAKEAWAYS:

1. Ms. Carmen Gonsalves, Head of International Cyber Policy at the Ministry of Foreign Affairs of the Netherlands, will depart her role as co-Chair of the GFCE on behalf of the Netherlands. The Netherlands will continue their role as co-chair of the GFCE.
2. Christopher Painter, President of the GFCE Foundation Board, spoke on the GFCE's priorities towards 2022: a demand driven approach; regional focus; and further developing the GFCE eco-system.

SUMMARY:

- Ms. Carmen Gonsalves delivered a speech to open the GFCE Consultation Meeting. The recognition of capacity building on the international stage is growing, and now more than ever it is important that well-equipped and resilient stakeholders work together to build and maintain an open, free and secure cyberspace. The GFCE should continue to grow as an inclusive, neutral, non-political network that is the venue of choice for all stakeholders to push forward the agenda for cyber capacity building.
- Christopher Painter, President of the GFCE Foundation Board, spoke on the GFCE's priorities towards 2022. He reaffirmed the GFCE's focus as first and foremost on facilitating the multi-stakeholder community, while expanding on the three (3) priority areas under this mandate: maintaining a demand-driven approach, increasing the GFCE's regional focus, and further strengthening this unique ecosystem.
- Additional priority areas endorsed by the participants included measuring and mapping cyber capacity at national and regional levels, ensuring that readily available existing capacities go to where they are needed, and encouraging knowledge transfer as part of the regional focus.
- The GFCE should focus on building a 'community of practice' of expert capacity builders. A better understanding of what does and does not work in CCB is necessary for championing new ideas and keeping up with evolving technologies.
- Participants also endorsed the GFCE's focus on inclusivity and enhancing collaboration. There was agreement that strengthening the GFCE brand will be an important element of the way forward for the GFCE. Regional liaisons can play an important role in ensuring the GFCE brand is accessible at all levels.
- One suggestion was to use the Research Agenda to explore whether the GFCE's strategic priorities align with national and regional cybersecurity strategies. With an initiative on regional hubs taking shape, this debate must extend beyond the GFCE Community.
- The GFCE should champion its unique position as the key multi-stakeholder player in this space, allowing it to connect countries to private sector and NGOs in various different ways.

From Negotiation to Implementation, the Importance of Cyber Capacity Building	Day	Session	Participants
⇧Top	1	2	135

SESSION OBJECTIVES:
During this session, GFCE Members and Partners had an opportunity to discuss possible ways that the GFCE could support the implementation of the United Nations Open-Ended Working Group (OEWG) & Group of Governmental Experts (GGE) outcomes on cyber capacity building and opportunities for GFCE engagement in the proposed OEWG Program of Action.

KEY TAKEAWAYS:

1. The GFCE is seeking to ramp up efforts in its aim to be the bridge between policy & practice. As the global platform for cyber capacity building, the GFCE should be part of institutional dialogues (like in the UN) & play a role in helping fill knowledge gaps and providing support in this area.
2. Regional meetings, such as the GFCE meeting in the margins of Singapore International Cyber Week in October, should be used to discuss input to the survey on implementation and coordination of outcomes from these institutional dialogues.
3. Mr. Secretary Ajay Prakash Sawhney, the GFCE co-Chair on behalf of India, mentioned that cyber capacity building needs scaling up. The GFCE should join hands with similar efforts at the UN as well as leverage digital means of consulting and communicating to derive best value from limited resources.

SUMMARY:

- After briefly reflecting on the recent conclusions of the UN OEWG and UN GGE, where several recommendations on what steps states can be taking to address capacity building were mentioned, panelists were asked to consider how should or could the GFCE be supporting the implementation of these outcomes.
- Given the outcomes of these important institutional processes, there is now a very strong normative framework that all UN members have agreed to and reaffirmed. Efforts by the multistakeholder community and the GFCE to do more on the implementation of this multilateral framework were welcomed.
- The final report of the UN OEWG also held consensus that states, on a voluntary basis, use National Survey of Implementation of UN General Assembly Resolution 70/237 as a model to help them inform the Secretary-General on their views, lessons learned, and good practices on capacity building. Input of Member States to this survey could also help the GFCE determine what the national CCB needs are.
- The GFCE could connect this survey with other sources of information on capacity needs and activities, such as Cybil and Cyber Maturity Models.
- The OEWG report lays out the principles of capacity building (para. 56), which will likely be the cornerstone of future references to cyber capacity building within the UN. Whilst there is no direct mention of the GFCE, there is some complementarity with the principles of the Delhi Communique.
- There is also value in approaches such as “adopt a norm”, where a few states adopt a part of the normative framework and share best practices. For example, The Netherlands aims to take a leadership role on CSIRTs and is working with international experts in a

multistakeholder setting to produce a Getting Started guide on establishing a CSIRT.

- Canada is running projects that aim to support state representation in institutional dialogues. They are working with organizations such as Cyber Law International and the Organization of American States to educate state representatives about developments in international law and building consensus amongst a more diverse group of stakeholders.
- There was endorsement for including stronger references to the GFCE in the context of institutional dialogues. The GFCE already has the foundation to lead cyber capacity coordination and there is room to expand on these efforts, which will hopefully lead to more states and other stakeholders becoming more closely involved in cyber diplomacy.
- Contextualizing terms such as norms and laws is important, especially in national contexts where English is not the first language, as these populations have a stake in these discussions. It is important that we contextualize these terms based on their own experiences rather than throw them into dominant narratives. One solution could be to develop multi-language reports.
- Whilst there are many existing capacity building initiatives, there is a need to assess and accurately map these efforts to make linkages between new norms and laws to the existing capacity. The UN recently launched its own database related to capacity building, though it was suggested that a resource in itself cannot replace mapping and matchmaking functions.
- An important first step is having the right people in the room. Discussions on norms & international law are being driven by foreign ministries and international legal experts, while the technical measures in government fall under other ministries. The GFCE can provide a platform for those communities to meet in the middle.
- Another suggested role for the GFCE would be to make connections with more diverse groups that can help support projects, as well as identify regional and national partners to improve understandings of who needs capacity building support.
- Some participants found it encouraging to see the efforts that the GFCE is already taking to bring in multiple stakeholders. More can be done to engage regional groups in terms of design and delivery of CCB programs.
- African nations in particular are experiencing capacity gaps across all themes. More support and assistance are needed for countries that do not have a law on cyber security to implement the international norms regarding cyber security. Cybil is an important tool and it would be useful to have this in multiple languages.
- Beyond CCB-related policy outcomes from the UN, greater coordination with regional and national agencies to provide country-level support to governments remains critical.
- Whilst the discussion focused primarily on dialogues in the UN First Committee, it is important to draw attention to other ongoing processes such as the Ad Hoc Committee on cybercrime and the Open-ended intergovernmental expert group.
- The GFCE could explore the idea of including a discussion on principles of CCB in the High-Level Conference on Capacity Building 2022. This could be the subject of a series of smaller consultations leading up to the conference.
- Research is currently underway on developing guidance for implementing cyber norms by showcasing numerous national examples, a project under the GFCE Global CCB Research Agenda 2021.
- The GFCE community should engage with institutional dialogues beyond the First Committee and ensure that efforts towards supporting states in practical implementation can be replicated inter alia in the context of cybercrime.
- The GFCE will be hosting a Southeast Asia Regional Meeting in the margins of the Singapore International Cyber Week Conference (SICW) in October 2021.

GFCE Clearing House Consultation Session	Day	Session	Participants
⇧Top	1	3	103

SESSION OBJECTIVES:
During this session a way forward for the GFCE Clearing House was discussed. Since 2018 the GFCE has provided a match-making function for member countries seeking international support to help address their capacity building needs.

KEY TAKEAWAYS:

1. In Q3 2021, the GFCE Secretariat plans to make additional capacity available for coordination of the clearing house mechanism, taking into account the feedback received from the GFCE Community. Tasks will include outreach and assistance on Clearing House cases.
2. A priority for the GFCE in developing its matchmaking function is articulating a demand-driven approach, whereby the needs of the recipient with regard to direct and indirect support are accurately identified and communicated. Until now, the process has focused heavily on existing supply, for example looking at what the Working Groups can provide to requesting Members.

SUMMARY:

- The aim of the GFCE Clearing House is to facilitate matchmaking between GFCE Members or Partners who have cyber capacity needs with those that can offer cyber capacity support.
- Prior and ongoing Clearing House cases in the GFCE include Tunisia, Sierra Leone, The Gambia and Senegal. Over the past 6 months the GFCE has been liaising with Papua New Guinea on support for developing their national cybersecurity policy.
- Simply defining where the demand is will not be sufficient. There should be a standard procedure for identifying and addressing this demand. The "full menu" should be publicly known, and all countries should be able to contribute equally.
- Identifying CCB demand & needs should be more accurate and in sufficient detail to identify an actionable, realistic, and feasible solutions (in terms of content, format and timelines).
- The GFCE also aims to scale up the clearing house process, expanding on a national approach – where each requesting country receives individual assistance – to include neighboring countries from the (sub)regional context in the process.
- Mapping activities amongst others through the AU-GFCE Project will contribute to a better understanding of national and regional CCB needs.
- The GFCE could develop other ways to survey the "CCB market" so the Clearing House can address the most important issues. In addition, as the Clearing House is a community-driven initiative, synergies should be built with and between the various GFCE pillars so everyone has a chance to contribute and ensure an optimal process.
- There should be more dialogue on the costs of capacity building support and where financing will come from.
- The clearing house process has proven lengthy in some cases, partially due to the requirement for formalities in the request and response. Action should be taken to manage expectations of how long clearing house cases might take.
- There is a need to ensure regional and local ownership of the work being done. Comprehensive outreach should be conducted from the outset with local communities and partner organizations to ensure that the approach and ecosystem is multistakeholder.

Showcase Catalog of Project Options for the NCS Cycle	Day	Session	Participants
⇧Top	1	4	101

SESSION OBJECTIVES:
The session represented the launch of the Catalog of Project Options for the NCS Cycle, developed by GFCE Working Group A Taskforce on Strategy & Assessments. The Catalog was showcased as an example of a Standard Support Package, which provides an overview of products and services that the GFCE can offer to its members, or which Members and Partners can offer to the wider community.

KEY TAKEAWAYS:

1. The GFCE Secretariat is developing an online version of the Catalog of Project Options for the NCS Cycle.
2. The Organization of American States will translate the Catalog into Spanish and Portuguese by August 2021.
3. The Catalog has led to additional projects such as the Global Overview of Assessment Tools (GOAT), which provides an overview of all existing cybersecurity assessments. The GOAT document is being translated into French and Spanish by the ITU.

SUMMARY:

- The Catalog aims to attract others to reach out to the GFCE and enable the Community to support those reviewing and developing cybersecurity strategies. The Catalog is intended to be a living document and continuously updated, not static in its current form.
- The idea behind the Catalog stems from a Member of Working Group A request for clarification on the types of assistance they might receive from the GFCE. After mapping the activities relevant to developing a cybersecurity strategy, it became clear that a Catalog would assist project managers in their own efforts.
- Five stages were identified in the development of a cybersecurity strategy. Volunteers were asked about their experiences and to elaborate on the possible activities within these five stages, building case studies around each stage.
- The various ways in which this Catalog could be utilized were highlighted. Firstly, the Catalog might be integrated into training materials for program and project design.
- Secondly, the tool might inform policy development inter alia by being used to look up ongoing updates and as a source of case studies or examples of cybersecurity strategy development (including regional examples).
- Finally, the tool might be used internally by the GFCE to identify knowledge gaps and possible new projects for the Working Groups or Task Forces.
- The Catalog has also led to a collaboration project with Working Group B to develop guidelines in bringing together existing knowledge, best practices & opportunities in identifying the needs and requirements for the process of identifying critical infrastructures (Critical National Infrastructure and Critical Information Infrastructure).
- The Task Force should consider targeted outreach on the Catalog to those who would be interested in the tool, such as policymakers, program managers & Clearing House candidates. The idea of producing a YouTube video on the Catalog was also mentioned.

Global CCB Research Agenda Consultation	Day	Session	Participants
⇧Top	1	5	92

SESSION OBJECTIVES:
During this session the progress and developments of the pilot Research Agenda were presented. In the breakout sessions, the GFCE community was encouraged to give input and share their thoughts on how they would like to be involved in the Research Agenda.

KEY TAKEAWAYS:

1. The Research Committee is currently reviewing the Research Agenda process. Input on the process, including feedback on collaborating more closely with the Working Groups, will be included in a revised Research Agenda process (envisaged Q3 2021).

SUMMARY:

- The Research Committee presented an update on developments of the Research Agenda process since its first iteration in late 2020. The Global CCB Research Agenda was developed as a tool by and for the GFCE Community to provide research outputs and data analysis for the wider cyber capacity community.
- Formed last August, the focus of the Research Committee is to support the development of the Research Agenda and liaise with the Working Groups to provide advice on research matters. Each Committee Member is assigned a Working Group or Task Force & the Committee meets regularly to discuss the Research Agenda.
- Since its launch the focus has been on testing the first Research Agenda through a community-driven process in four phases: 1) Fifteen ideas were identified in the Working Groups and then refined prior to the Annual Meeting 2020, 2) GFCE community voted on ideas during an agenda-setting exercise and ideas were ranked and presented in the Research Agenda, 3) The ideas that received the most votes were prioritized for funding and the research was commissioned, and 4) Research projects are underway and will conclude by October 2021.
- The Research Committee recently convened during a virtual retreat to reflect on lessons learnt so far, based on engagement with the Community and ongoing research projects.
- Whilst the Research Agenda is a great bottom up GFCE tool, additional ideas from other communities should also be welcomed (e.g. through engaging academic researchers).
- The Working Groups & Task Forces should spend more time discussing and identifying the knowledge gaps that are most important to them. Scoping is also important to validate research ideas but there must be a balance with the work and needs of the Community.
- One suggestion was to create a dashboard of the scoping to explain how an idea would be circulated and how it would be framed within the strategy of both the GFCE and the Working Groups.
- To engage the GFCE community in the prioritization of ideas, the Research Committee could survey the GFCE members on what the knowledge gaps are, and could also provide insights on engagements with global thought leaders to share perspectives on useful research that can be conducted.

GFCE & Pacific Region	Day	Session	Participants
⇧Top	2	6	51

SESSION OBJECTIVES:
This session followed up on previous engagements at the GFCE Regional Meeting in Melbourne (February 2020) and the GFCE Annual Meeting (November 2020). Led by GFCE Pacific Liaison Cherie Lagakali, and substantiated by outreach conducted with Pacific stakeholders, the GFCE has been drafting a scoping report analyzing the possibilities for a sustained GFCE presence in the Pacific region. The findings of the scoping report were presented here.

KEY TAKEAWAYS:

1. Once a recommendation on a GFCE presence in the Pacific is presented to the GFCE Community and engaged Pacific island stakeholders in Q4 2021, the aim is to begin establishing this GFCE presence by the end of the year.

SUMMARY:

- Key analysis finding: The concept of cyber capacity building (CCB) is not sufficiently defined. This makes a common understanding of CCB difficult to reach amongst Pacific Island stakeholders.
- Key analysis finding: Shortened projects with limited scopes and low impact are a reality in the Pacific region. This indicates that the modalities and types of CCB assistance need to evolve.
- Contextualization and culture are important. The findings of the report underpin the need to employ solutions to the coordination of CCB in the region that are sensitive to the way the Pacific is doing things.
- A GFCE presence in the region should be built around a mandate that is collaborative, inclusive, meets stakeholder needs and puts them first.
- **GFCE Pacific Mission Statement:** “To create stronger Pacific cyber capacity building communities, structures and approaches that make cyber capacity building efforts more concerted, more fit-for-purpose and more resourceful, in a manner that is Pacific appropriate, Pacific sensitive, and done the Pacific way.”
- There are challenges to the identification, design, and implementation of CCB efforts in the Pacific, where issues related to transparency, setting objectives, and local ownership frequently arise.
- Ultimately the aim of this scoping exercise is to find the best model for Pacific island countries to coordinate, collaborate, and share information with each other on cyber capacity building. This is encapsulated in the GFCE Pacific Mission Statement.
- The speakers outlined the scoping findings and presented (1) the landscape of venues for discussions on ICT issues and cyber capacity building, (2) operational needs for CCB, as well as (3) the mandate options for a GFCE presence in the Pacific.
- It is important to create strong Cybersecurity communities and niche capacities/expertise among economies in the Pacific. It is currently difficult to share resources and capacities amongst countries in the region, especially when considering the geographic reality.

- For the Pacific, security and development are the main agenda items. The support from the GFCE seems to capture this well.
- Opening a physical office in the region could help build trust with local stakeholders, as it is more accessible and permanent in nature.
- Resource constraints should be considered when trying to establish a GFCE presence in the region. Beyond time and money, commitment is also an issue - setting clear roles and responsibilities would help justify and cement these efforts, whilst reducing the potential for duplication.
- One of the main considerations for the GFCE is that there is added value for the Pacific community, and that interventions are led by the needs of the environment.
- Pacific island Members were encouraged to think about cybersecurity capacity from the policy and strategies perspective, where CCB is an emerging and evolving field. As best practices evolve, especially in terms of how CCB links to development, there are opportunities for countries to feed into discussions & thinking at the global level based on practical experiences.
- The mandate options look promising for supporting both those economies that are in the initial stages of development and those who are leading cybersecurity support in the region.
- In Fiji, government and the private sector are working separately in the provision of capacity building. Some encouragement for collaboration between these stakeholder groups is key. This is a prerequisite for bilateral and multilateral collaboration.
- There is a lot of work currently being done in the Pacific at all levels and on all themes. Taking a broad approach to the project might help capture all that good work and achievements thus far, reaching a broader range of partners.
- There is also a need to allocate sufficient resources and capacity to the project if it is to have the necessary expertise and advocacy to strengthen all these engagements, as well promote the involvement of local experts and professionals in the process.
- It may be advisable to start with modest goals so that the presence can grow with the capacity and needs.
- There was strong sentiment that any approach of the GFCE should remain aware of and not affect existing programs that those on the ground have planned for this year.
- Further elaboration on how the mandate options would be operationalized would be valuable, especially if moving forward with a more ambitious mandate. This would outline how the proposed mandate might affect the day to day of those on the ground, creating harmony with the work they are doing and preventing duplication.
- It would be good to see GFCE play more of a role in contextualizing the global context, as this is useful for governments focused primarily on issues of national or regional security and stability. With each nation drafting its own security agenda it would be very useful to understand how this can be mapped or operationalized in relation to CCB. Any strategy or policy derived from this would inherently be drawn from a national security policy, empowering small nation countries to identify where global context fits in their agenda.
- Clarification was sought on references to collaboration between Pacific island countries, and which stakeholders this engagement would focus on. The project aims to be as inclusive as possible of all stakeholders. Whilst many of the capacity building initiatives discussed during outreach have been in the context of providing support for national capabilities, this does not preclude a more multistakeholder effort.

GFCE Engagement on Cyber Capacity Building in Africa	Day	Session	Participants
⇧Top	2	7	85

SESSION OBJECTIVES:
During this session the GFCE aimed to outline possible modes of engagement and solicit feedback from the GFCE Community regarding the proposed plans and activities for both the GFCE Africa Strategy and the AU-GFCE Collaboration Project.

KEY TAKEAWAYS:

1. Invitations will be sent out to participants of the GFCE Africa Regional Dialogue.
2. There will be an open call for contributions from the GFCE Community to the GFCE knowledge modules. Feedback will also be requested on the draft outline mapping of national CCB needs.
3. The GFCE should continue to collect information about CCB projects to deconflict and coordinate ongoing efforts. Analytical summaries of key CCB focus areas could build on tools like Cybil and help stakeholders navigate a crowded & complex landscape.

SUMMARY:

Keynote

- As highlighted by the keynote speaker, we are increasingly exposed to threats in our digitalized world. Global multistakeholder collaboration is needed now more than ever to confront these threats, ensuring that Africa does not become a weak link but has the requisite capacity to bring its unique value to the world.
- The keynote speech touched on the links between cyber capacity building as an issue not only of security but also one of economic and social development. Solutions should not only focus on risk management but should also be people centric, empowering digital Africans as much as improving the digital environment in which they can thrive.

GFCE Africa Program

- The GFCE's strategy under the Africa Program was presented. This strategy is underpinned by a thorough understanding of the Africa landscape, consolidated in a mapping exercise.
- The various entities and institutions focusing on CCB in the region include the African Union (AU) Commission, AU Development Agency, Regional Economics Communities (REC), African Capacity Building Foundation, and the African Development Bank.
- The African Union Digital Transformation Strategy 2020-2030 provides a very favorable environment for linking CCB with the development agenda on the African continent.
- The African Union Development Agency (AUDA-NEPAD) is to become a GFCE Member. The GFCE currently counts 16 African Union Member States and 2 RECs as part of its community. Seven of these Members and Partners have joined since March 2021.
- The overall outreach will incorporate an inclusive, multistakeholder approach to achieve and implement the strategy. The aim is to work closely and directly with AU

Member States, RECs, and the AU organs, building synergies with the GFCE Secretariat and the AU-GFCE Collaboration project.

- The program includes four lines of action:
  - **Outreach & Branding of the GFCE**: Establishing a critical mass of African GFCE Members and Partners & promoting the GFCE within the continent.
  - **Build an African GFCE Community**: Creating a strong network of African stakeholders that contribute to the CCB agenda in Africa, with a particular focus on animating the Africa Group on Cybersecurity and African Women on Cybersecurity.
  - **Coordinate CCB Activities within the African Region**: Working with all institutions engaged in CCB activities in Africa & supporting the AU-GFCE collaboration project.
  - **Support and Strengthen CCB Implementation**: Promote and connect those within the African region with the GFCE ecosystem, making use of Cybil, other GFCE tools and the Working Groups.
- Considering the challenge of bureaucracy in African organizations, it will be increasingly important to connect with the right actors within institutions capable of driving these projects forward. This aspect is incorporated in the landscape mapping.

African Union-GFCE Project

- The AU-GFCE Project aims to enhance existing knowledge on CCB topics, helping AU Member States identify and prioritize their needs in enhancing national cyber capacities and resilience. Through this collaboration it is also envisaged that engagement of and with African nations within the GFCE will be improved.
- Over its two-year duration, the project aims to deliver in three key areas:
  - **Mapping cyber capacity building needs.** This involves carrying out a baseline gap analysis. The mapping will result in a consolidated overview of existing resources, beginning with the core themes under the Delhi Communique and tracking the status of CCB of African nations through various sources, such as assessments, validation exercises and direct outreach.
  - **Establishing an African Cyber Experts (ACE) Community.** Experts will be put forward by participating AU Member States and other African Union affiliates. Representatives put forward for selection would come from government, CERTs/CSIRTs, and the civil society sector.
  - **Developing GFCE knowledge modules.** To support the overall objectives of this project, the aim of this deliverable is to make use of existing knowledge combined with the expertise, tools & other resources that GFCE Members and Partners have on key CCB topics.
- Knowledge modules must be connected to policymakers at both the national and continent levels.
- It is important to coordinate with other actors, especially those organizing events, to save resources, avoid duplication and make connections between networks.
- Protection Group International are working with the United Kingdom on the African Cyber Fellowship. This could be source of learning for the GFCE's engagements in Africa.
- The project aims to bring benefits to both the GFCE and African communities. For African stakeholders this would mean not only a better understanding of national priorities according to needs, but also improved engagement and means of addressing CCB challenges with local ownership and sustainment.

- For the GFCE Community, a better understanding of national priorities and CCB needs in Africa could enhance cooperation and knowledge-sharing on CCB initiatives and activities between donors, recipients & implementers. The project is also a chance to demonstrate knowledge and expertise of GFCE Members & Partners, inter alia through the knowledge modules.
- CERTs and governments have been considered separate actors for the purposes of the Africa Cyber Experts Community. This recognizes of the distinct roles, capabilities and expertise of these actors. Governments will be asked to provide recommendations of experts from CERTs.
- Input from the GFCE Working Groups, the African Cyber Experts Community, the African Union Cyber Security Experts Group, and the mapping of national cyber capacity needs will all contribute to the knowledge modules.
- There is also an intention to develop knowledge modules on “Communicating the impact of CCB” and on “Bridging the gender gap in cybersecurity leadership.”
- There should be more engagement with the GFCE Working Groups to improve awareness on the AU-GFCE Project and help WG Members understand how they can become more involved.

GFCE & Europe Region	Day	Session	Participants
⇧Top	2	8	67

SESSION OBJECTIVES:
This session focused on cyber capacity building trends and developments in the Europe region, with speakers presenting their global initiatives and insights to the Community.

KEY TAKEAWAYS:

1. The EU and its partners have made various initiatives aimed at enhancing synergies and collaboration amongst global stakeholders and creating change at the policy-level.
2. Effective CCB coordination is ultimately an exercise of transparency amongst cyber capacity builders.

SUMMARY:

- In December 2020, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy published a joint communication on the EU's cybersecurity strategy for the digital decade.
- In March 2021, the Council adopted conclusions on the cybersecurity strategy, highlighting a number of areas for action in the coming years, including on proposals for a EU Capacity Building Agenda, the establishment of an EU Cyber Capacity Building Network and the need for all partners to work together to ensure coordination and reduce duplication.
- The Global Trends Report finds that while the field of CCB is expanding, professionalizing, and maturing, implementation still lags behind. The report underscores the importance of coordination as it recommends that we support coordination in countries with numerous projects particularly in Eastern Europe and the Western Balkans.
- Effective CCB coordination is:
  - **Characterized by transparency.** It goes deeper than merely exchanging information; it is about adapting individual workplans and calendars to become more open and flexible in enabling synergies with fellow capacity builders. In addition, effective CCB coordination involves the freedom to choose actors to work with – not to be the 'only player in the game'.
  - **Conducted at the country-level.** This type of coordination paves the way for all involved stakeholders (e.g. donors, implementers, and recipients) to convene, discuss specific needs and priorities, and identify opportunities for synergies accordingly.
  - **Led by recipients.** CCB coordination must be an effort of donors, implementers, and recipients with recipients (the beneficiaries) in the lead; however, this type of coordination may be difficult as there may be a lack of strategic leadership and resources in recipient countries. This can be addressed by engaging recipients in needs assessments, guiding them through the process, offering tool assistance, and encouraging them to say 'no'.
- Cybersecurity naturally fosters multistakeholder collaboration in which diverse actors are brought together to develop inclusive solutions that are practical and beneficial for all; however, dedicated government actions by EU institutions and their member states

to formalize cyber multistakeholderism (e.g. operationalizing a multistakeholder model) remain rare despite them constantly engaging in discourse.

- To mitigate or adapt to the afore mentioned CCB trends within Europe and the globe, the following initiatives have been or are being conducted:
  - **Cybersecurity board and agenda by the EU.** Realizing the growing number of actors and projects in CCB as well as the importance of effective coordination, the EU is in the process of setting up a Cybersecurity board and agenda purposed to enhance synergies and identify priorities. As the work of the EU is global in nature, cyber diplomacy is utilized as a tool to involve various actors (e.g. regional organizations, cyber attaches and delegations, policymakers, etc.) in their work through high-level discussions, networks, and training sessions.
  - **European Cyber Agora.** Given the lack of formalized and institutionalized multistakeholder collaboration at the policy-level, the European Cyber Agora aims to encourage more multistakeholder dialogue in CCB through workshops tackling a range of topics from building the CyberPeace index to bolstering the protection of human rights online through the EU's cyber diplomacy efforts.
- Whilst the field of CCB is expanding, with the list of actors and projects growing and multistakeholder discussions becoming more prevalent, implementation and dedicated government actions on formalizing cyber multistakeholderism lag behind.
- The community has been invited to join the European Cyber Agora and propose workstreams/workshops. Previous workshops can be accessed and viewed here. Another call for participation in upcoming workshops will be sent later this year to capture different voices and perspectives across Europe.

GFCE & LAC Region	Day	Session	Participants
⇧Top	2	9	65

SESSION OBJECTIVES:
The aim during this session was to present recent developments and best practices on Cyber Capacity Building (CCB) in Latin America and the Caribbean (LAC). Panelists presented four major initiatives that will shape cyber capacity building in Latin America in the coming years.

KEY TAKEAWAYS:

1. With cybersecurity strategies becoming more complex, there is a need for initiatives and projects to be modelled around the cyber capacity needs in the LAC region. This must be a shared responsibility and the region must capitalize on partnerships to bridge gaps.
2. There are multiple ongoing initiatives in the LAC that aim to enhance knowledge-sharing in the community, provide support and assistance, trainings, and foster public-private partnerships to enhance cyber capacity building within the region.
3. It is of importance to understand the gaps and needs of different sectors and infrastructure within the LAC community in order to develop the right tools and training initiatives suitable for LAC needs and priorities.
4. In order to enhance regional cyber capacity, there is a need for fostering dialogue and cooperation between all relevant stakeholders, including enhancing public and private partnerships.
5. There needs to be a facilitation of conversation and cooperation within the multistakeholder community on highlighting the needs and demands on a regional and stakeholder-level, which the GFCE could play a role in facilitating.

SUMMARY:

- There are multiple ongoing initiatives in the LAC region that were presented:
    - The EU CyberNet initiative is a community of knowledge-sharing comprised of a tool of trainers that aims to develop cybersecurity skills and expertise as a 'one-stop shop' for EU expertise in providing global technical assistance. The EU will also launch a regional CCB center in the Dominican Republic which will be involved in a multitude of cyber initiatives and owned by the region. The center will cater to regional needs and nurture expertise by teaming up with regional organizations and building on their input.
    - The IADB has been offering support and assistance on the digital development of the LAC region. The IADB has fostered digital government operations, offered assistance and support in providing training initiatives, publications and studies on a wide range of sectors to assist countries in the region to use their resource to improve their cyber capabilities.
    - ARIN is developing human resource development initiatives focusing on network operators to provide technical capacity programs for this group. The program would not only cover technical information, but also more policy-based issues. The program is also collaborating with local universities in order to provide certification procedures for those in the field. ARIN initiatives in the region also include securing

    critical infrastructure by developing training and best practices on understanding emerging gaps and developing best practices on coordination.
  - CISCO and the OAS are developing a partnership in order to, amongst other objectives, foster alliances, develop cybersecurity skills and drive innovation in Latin America. Some of the initiatives include the development of a Cybersecurity Innovation Concepts tool, an innovation fund, partnerships with various nations, and setting up trainings and various activities.
- There is a need to understand the needs of different sectors and highlighting the gaps and priorities to provide a stronger basis for training and capacity building.
- The development of CCB in the region is a challenge, partly due to the skills gap alongside the difficulty in retaining cyber professionals within the LAC region. It is important to develop cyber skills and awareness both to governments and policymakers, alongside creating an educational track for cyber careers.
- Enhancing public and private partnerships in the region is significant alongside connecting to other stakeholders and the wider community to participate in initiatives.
- Cybersecurity is a team effort and both the private and public sector should play a role in supporting the skills gap development, such as developing trainings and educational tracks as well as supporting women in developing cyber skills.

Opening GFCE Consultation Meeting & Strategic Way Forward

Tuesday 15 June, 12:00-12:45 UTC

Carmen Gonsalves

Head of International Cyber Policy, Ministry of Foreign Affairs of the Netherlands & Co-Chair, Global Forum on Cyber Expertise

Christopher Painter

President of the Foundation Board, Global Forum on Cyber Expertise

From Negotiation to Implementation, the Importance of Cyber Capacity Building

Tuesday 15 June, 12:45-13:30 UTC

Elina Noor

Director, Political-Security Affairs & Deputy Director, Washington D.C. Office, Asia Society Policy Institute

Joyce Hakmeh (MODERATOR)

Senior Research Fellow, Chatham House

Kaja Ciglic

Senior Director for Digital Diplomacy, Microsoft

Nathalie Jaarsma

Ambassador at-Large for Security Policy and Cyber, the Netherlands

Nick Natale

Senior Project Manager, Anti-Crime Capacity Building Program, Global Affairs Canada

GFCE Clearing House Consultation Session

Tuesday 15 June, 13:40-14:10 UTC

Manon van Tienhoven (MODERATOR)

Program Coordinator, Global Forum on Cyber Expertise

Daniela Schnidrig

Cybersecurity Capacity Building Programme Lead, Global Partners Digital

Hein Dries

Key Expert Cybercrime, West African Response on Cybersecurity and Fight against Cybercrime (OCWAR-C)

Moctar Yedaly

Africa Program Manager, Global Forum on Cyber Expertise

⇧Top

Showcase Catalog of Project Options for the NCS Cycle

Tuesday 15 June, 14:10-14:40 UTC

Carolin Weisser Harris

Lead International Operations, Global Cyber Security Capacity Centre (GCSCC)

Lea Kaspar (MODERATOR)

Executive Director, Global Partners Digital (GPD)

Robert Collett

Researcher & Consultant

Global CCB Research Agenda Consultation

Tuesday 15 June, 14:40-15:10 UTC

Andrea Calderaro

Senior Lecturer/Associate Professor in International Relations & Director of the Centre for Internet and Global Politics, Cardiff University

Carolina Aguerre

Senior Research Fellow (in Residence) of the Center for Global Cooperation Research, University of Duisburg-Essen

Enrico Calandro (MODERATOR)

Co-Director of the Cybersecurity Capacity Centre for Southern Africa (C3SA), University of Cape Town

Richard Harris

Principal Cybersecurity Policy Engineer, MITRE

GFCE & Pacific Region

Wednesday 16 June, 05:00-05:45 UTC

Bart Hogeveen

Head of Cyber Capacity Building, International Cyber Policy Centre, Australian Strategic Policy Institute (ASPI)

Cherie Lagakali

Secretary, Pacific Island Chapter of the Internet Society (PICISOC) & Pacific Liaison, Global Forum on Cyber Expertise

Thomas Jordan

Senior Advisor and United Kingdom Liaison to the Global Forum on Cyber Expertise

⇧Top

GFCE Engagement on Cyber Capacity Building in Africa

Wednesday 16 June, 13:00-14:30 UTC

Abdul-Hakeem Ajijola

Chair, African Union Cyber Security Expert Group

Martin Koyabe

Senior Manager AU-GFCE Collaboration Project, Global Forum on Cyber Expertise

Moctar Yedaly

Africa Program Manager, Global Forum on Cyber Expertise

Towela Nyirenda-Jere (MODERATOR)

Head of the Economic Integration Division, African Union Development Agency (AUDA-NEPAD)

GFCE & Europe Region

Wednesday 16 June, 14:40-15:25 UTC

Franziska Klopfer

Project Coordinator, Europe and Central Asia Division, Geneva Centre for Security Sector Governance (DCAF)

Manon le Blanc

Head of Cyber Sector, EU Diplomatic Service, European External Action Service (EEAS)

Nikolas Ott

Project Manager for Cybersecurity Policy and Digital Diplomacy, Microsoft

Patryk Pawlak (MODERATOR)

Brussels Executive Officer, European Institute for Security Studies (EU ISS)

Robert Collett

Researcher & Consultant

GFCE & LAC Region

Wednesday 16 June, 15:25-16:10 UTC

Bevil Wooding

Director of Caribbean Affairs, American Registry for Internet Numbers (ARIN)

Kerry-Ann Barrett (MODERATOR)

Cyber Security Policy Specialist at the Cyber Security Program, Organizaton of American States (OAS)

Liina Areng

Regional Programme Lead, EU CyberNet

Mario de la Cruz Sarabia

Senior Director of Public Policy & Government Affairs, Cisco Latin America

Santiago Paz

Cybersecurity Sector Specialist, Inter-American Development Bank