GFCE ANNUAL V-MEETING 2021 | REPORT

Table of Contents

Report on the GFCE Annual V-Meeting 2021 3

DAY 1: Strengthening our Demand-Driven Approach 5

DAY 2: Stocktaking the GFCE Supply Side 9

DAY 3: Bridging Demand and Supply for Cyber Capacity Building 12

GFCE Deliverables presented at the Annual V-Meeting 2021 16

Program & Speakers Overview 17

Report on the GFCE Annual V-Meeting 2021

Strengthening the GFCE's Demand-Driven Approach

The Global Forum on Cyber Expertise (GFCE) has evolved into a diverse and global multistakeholder community of more than 140 Members and Partners. Every year, the GFCE hosts the Annual Meeting bringing together the GFCE community to discuss achievements and common objectives in determining the future of the GFCE and its work on Cyber Capacity Building (CCB).

In 2022, the aim is to bridge the gap between cyber capacity building demand and supply. This entails strengthening the GFCE's demand-driven approach focused on accurately defining needs, stocktaking the existing supply of cyber capacity building, and addressing any gaps. Based on this ambition, the theme of this year's Annual Meeting was: "Strengthening the GFCE's Demand-Driven Approach".

The GFCE Annual V-Meeting 2021 took place virtually on our online event platform, with more than 250 participants joining us for a three-day journey on cyber capacity building. In this report, you will find a summary of the sessions held at the Annual V-Meeting 2021, the recordings of the sessions, high-level cyber capacity building reports and an overview of GFCE deliverables in 2021.

DAY 1: Strengthening our Demand-Driven Approach

The first day had a regional focus, discussing regional cyber capacity building needs and what the GFCE has done thus far in identifying these and steering its work from the demand side:

Opening Session	Report	Recording
Regional CCB Priorities	Report	Recording
Strengthening the Demand-Driven Approach in Africa	Report	Recording
Integrating Cyber Capacity Building into the Digital Development Agenda	Report	Recording

DAY 2: Stocktaking the GFCE Supply Side

The second day highlighted the strong foundation that the GFCE has built over the past six years by stocktaking the supply side of cyber capacity building within the GFCE:

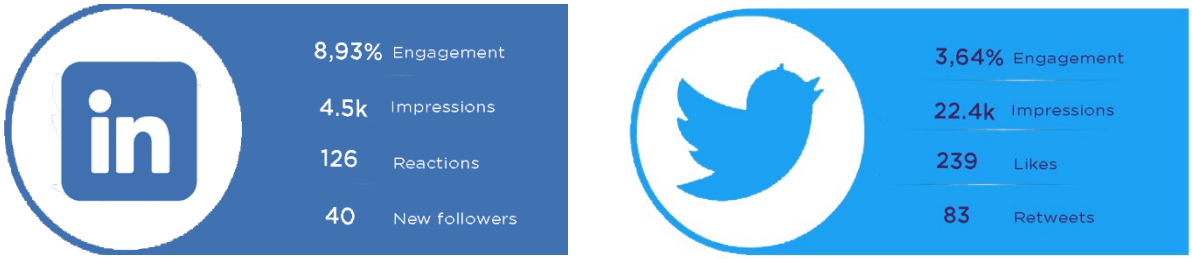
Asia-Pacific: Recipes for Good Cyber Capacity Building	Report	Recording
Stocktaking the GFCE Supply Side	Report	Recording
Collaborating on CCB – What do the GFCE Working Groups have to Offer?	Report	Recording
Refining the GFCE Knowledge Sharing Tools	Report	Recording

DAY 3: Bridging Demand & Supply for Cyber Capacity Building

The third day focused on bridging demand & supply for cyber capacity building, looking at the need for a strong and more efficient focused cooperation to further adopt a demand-driven approach:

Reflecting on Global Trends and Developments in Cyber Capacity Building	Report	Recording
Raising the Stakes in Cyber Capacity Building	Report	Recording
Multistakeholder Reflections on the Way Forward	Report	Recording
Closing Ceremony	Report	Recording

Annual V-Meeting 2021: numeral overview



Annual V-Meeting 2021: Social Media engagement

6 deliverables were presented during the Annual V-Meeting 2021

DAY 1: Strengthening our Demand-Driven Approach

Opening Session

The GFCE Annual V-Meeting 2021 opened with a panel discussion on how global cyber capacity building (CCB) efforts, and specifically those of the GFCE, can be strengthened by a demand-driven approach.

Chris Painter, President of the GFCE Foundation Board, highlighted that the cornerstone of the GFCE has always been the needs of the community. Throughout its formative years, the GFCE needed to build a solid foundation of knowledge and resources. During this time, the ecosystem of the GFCE evolved in response to what individual Members and Partners had to offer, in addition to considerations of how the GFCE could provide a platform to foster the sharing of expertise and best practices on the supply-side. The GFCE's regional efforts throughout 2021 have enabled a better understanding of local contexts and have highlighted the importance of listening to local needs. This is why, in 2022, the aim is to strengthen the GFCE's demand-driven approach by focusing on accurately defining needs through a regional approach, stocktaking the existing supply that the GFCE community has to offer, and address gaps to the GFCE community. Another ambition for 2022 is to co-organize a High-Level Cyber Capacity Building Conference with the World Bank, CyberPeace Institute, and the World Economic Forum which will elevate high-level political awareness of cyber capacity building. The conference will be held in Washington and hosted by the World Bank.

Maartje Peters was announced as the new GFCE Co-Chair on behalf of The Netherlands. Moving forward, Maartje sees a role for the GFCE in amplifying its efforts at supporting coordination and sharing knowledge amongst cyber capacity building practitioners by strengthening the connections with regional liaisons and hubs, leading local coordination networks in a few priority countries and expanding the Cybil Knowledge Portal. Moreover, Maartje highlighted that The Netherlands has been supporting the GFCE with core funding since its creation in 2015 and urges other GFCE members to provide their support as well, in order to collectively facilitate the GFCE's demand-driven approach and to keep expertise and knowledge within the GFCE community free and available for all.

Ajay Prakash Sawhney, GFCE Co-Chair on behalf of India, agreed that strengthening the demand-driven approach of CCB is a priority for the field. Moreover, he echoed the significance of a regional focus within this demand-driven approach. He stressed that regional meetings are used to help facilitate GFCE member countries in identifying and working towards fulfilling their CCB goals.

Joanna Kulesza, Co-Chair of the GFCE Advisory Board, stressed the importance of a civil society perspective in strengthening the demand-driven approach. She looks forward to engaging with civil society organizations that are GFCE partners and reaching out to new civil society organizations within academia, NGOs, and beyond, to help the community better address local and global challenges.

Regional Cyber Capacity Building Priorities

Over the last two years, the need for a regional approach to CCB has become undeniable and will be instrumental in improving collaboration and knowledge sharing amongst stakeholders. GFCE regional meetings were held in Europe, Southeast Asia and Latin America and the Caribbean, Africa and the Pacific across 2021. These events have brought together stakeholders to discuss issues, learn from each other and find solutions to capacity building challenges. In this panel discussion, representatives from the different regions provided updates on the GFCE regional meetings and discussed priorities. The session was moderated by ***Folake Olagunju*** from ECOWAS.

Manon Le Blanc, representing the European External Action Service, provided a European perspective. The EU began investing in CCB in 2010 and released its first cybersecurity strategy in 2013, implementing numerous programs on tackling cybercrime, training judicial and law enforcement authorities, and establishing CERTS. Amongst its CCB priorities, the EU has highlighted the need to enhance bilateral relations, including with key African partners, and support the implementation of CCB activities across the cyber domain. To do so, in the EU Cybersecurity Strategy in 2020, a proposal for a cyber security capacity board and a CCB agenda was put forward which would allow for increased effectiveness of the EU's approach.

The next panelist, ***Ka Man Yip*** representing Singapore, shared perspectives from the ASEAN region. Since 2016 the Cyber Security Agency of Singapore has been committed to the implementation of CCB projects and in 2021 the ASEAN-Singapore Cyber Security Centre of Excellence was established. In October 2021, the first GFCE-SE Asia Regional Meeting was held, bringing together regional stakeholders to discuss priorities and challenges on CCB and how the GFCE can play a coordinating role. It was highlighted that the region needs to have a clear picture of the CCB gaps in order to foster closer cooperation between stakeholders. Thus, the GFCE is in a global position and can help the region identify CCB priorities, fostering regular regional discussions.

From the LAC region, ***Kerry-Ann Barrett*** shared experiences from the Organization of American States (OAS) as the GFCE Regional Hub. The first regional meeting was held in March 2021, with a first introduction for the LAC Community to the GFCE, positioning the OAS as the link between the GFCE and the regional stakeholders in the Americas. In November 2021, the hub recognised the need to bring together donors and implementors in CCB and hosted a second regional meeting to discuss how the GFCE-OAS hub can better coordinate these actors. Based on the discussions, it was highlighted that the GFCE-OAS hub can play a crucial role in coordinating the various regional players, bringing experience from the global to regional level.

Bringing new perspectives on regional CCB priorities, ***Dr. Towela Nyirenda-Jere*** from AUDA-NEPAD talked about how the GFCE is supporting CCB initiatives through the AU-GFCE Collaboration Project that helps countries identify their CCB needs. Some of the benefits brought to the region from this project are: the targeted approach on helping countries identify specific CCB needs, the development

of a regional community of cyber experts, and the strengthening of knowledge available to the region. To coordinate activities across the continent, the GFCE established the African CCB Committee and is also supporting the establishment of the African Network for Women in Cybersecurity to empower female experts of the region and connect them with others globally.

The final regional priorities were shared by the GFCE Pacific Liaison, ***Cherie Lagakali.*** In February 2020 the first GFCE Pacific regional meeting was held in Melbourne, during which the regional community called on the GFCE to support coordination and collaboration and improve the design of CCB efforts in the region. For this reason, the GFCE commissioned a scoping regional assessment and a proposal for establishing a GFCE Pacific Hub with the aim to create stronger CCB communities to make CCB efforts more Pacific-sensitive. The GFCE Pacific hub will be incorporating regional players in the planning process which will be done by having products, advice, stakeholder engagement and activities by ensuring coordination and knowledge sharing.

As highlighted, regional organizations have a clear overview of CCB needs and priorities and it is crucial to be able to work and collaborate with the GFCE, as the latter can help translate needs in specific activities and provides access to a global multistakeholder community that is constantly sharing lessons learned and best practices from different regions.

Strengthening the Demand-Driven Approach in Africa

The region that the GFCE was most involved in throughout 2021 and has high ambitions for is the African region. This session, moderated by ***Moctar Yedaly***, elaborated on how the GFCE is strengthening its demand-driven approach in this region through the AU-GFCE collaboration project and the facilitation of the Africa Cyber Capacity Building (CCB) Coordination Committee. The AU-GFCE collaboration project aims to enhance African countries to better understand cyber capacities and identify and address their national cyber capacity needs. The project has 3 objectives:

- Conduct an assessment of the CCB needs and where countries are in their cyber capacity
- Form the Africa Cyber Experts (ACE) Community
- Develop knowledge modules (KMs) about how to understand and address cyber capacity challenges and needs

As highlighted by ***Dr. Towela Nyirenda-Jere*** from the AUDA-NEPAD, for the African countries, the project emphasizes the support to member states for capacity building initiatives, creating a link between strategy and implementation. Although the African region has strategies related to cyber capacity building, there are difficulties when it comes to implementation because of the rapid pace of digital developments and the lack of adequate investments in capacity building initiatives. The project can thus enhance sharing cyber capacity knowledge within the continent from areas with high supply to areas with limited capacity and expertise.

Dr. Martin Koyabe, representing the GFCE, highlighted that the AU-GFCE project team has interacted with several African countries which have identified priorities aligning them with the five thematic priorities of the GFCE based on the Delhi Communique. During this process, it has been highlighted that it is important to bridge the global and regional levels on CCB with the national level, making sure that

the outcomes of the project are contextualized based on national CCB needs. Another key point stressed is the need to ensure a bottom-up process on setting CCB needs and priorities, a process which the GFCE coordinates, bridging demand and supply in CCB.

Moving forward in 2022, the newly established Africa CCB Committee will help with the sustainment of the project ensuring that the outcomes are utilized efficiently. To achieve this, it is important to ensure the involvement of the multistakeholder community from the African Cyber Experts (ACE) Group and the Africa CCB Committee. As highlighted by the panelists, the AU-GFCE collaboration project demonstrates that the approach the CCB community should be taking, is to make sure that countries' needs are identified and they are involved in the decision-making process. The AU-GFCE project also helps African countries to interact with the GFCE community and make use of the GFCE Tools, bringing national and regional findings to the global context.

Integrating Cyber Capacity Building to the Digital Development Agenda

This session was dedicated to the official release of the GFCE Report: **"Integrating Cyber Capacity to the Digital Development Agenda."** The report, conducted by ***Melissa Hathaway*** and ***Francesca Spidalieri*** and supported by the World Bank's Digital Development Partnership (DDP), intends to identify pathways to bridge the broader development community to the cybersecurity capacity building (CCB) community and recommend effective mechanisms to incorporate cybersecurity into digital development projects and initiatives. A panel discussion took place with ***David Satola***, ***Vladimir Radunovic***, ***Kerry-Ann Barrett***, ***Kanwaljit Singh***, moderated by ***Patryk Pawlak***.

Since its establishment in 2015, the GFCE recognized the need to raise cybersecurity and capacity building as topics to be included in the national digital agenda of countries. Based on this, the project's objective was to examine how to better align the two communities by identifying best practices, highlighting key challenges and benefits of incorporating cybersecurity, digital resilience and capacity building into the development agenda as well as bridging venues and activities that could facilitate a tighter alignment and collaboration between the capacity building and the digital development communities. As the result of significant contributions from across the broader multistakeholder digital development and cybersecurity communities, the report identifies a number of striking findings amongst which are: the need to adopt a common definition of capacity building, the understanding that cybersecurity and digital resilience are still not seen as strategic cross-cutting issues, the need to understand that cyber security is not only about security but also about resilience, safety, sustainability, human rights. The report also highlights the need to build on cyber security workforce and develop indigenous capacity; make career pathways clear, provide specific education in schools and university, develop tailored made programs based on local needs.

As agreed by all panelists, the outcomes of the report will give concrete input for a dialogue as a new starting point of a process, which will bridge the gap between the development community and cyber security capacity building community, running up to the High-Level CCB Conference taking place next year. Bridging the cyber capacity building and the development communities will have numerous of benefits to both sides, as digitalization has become one of the most important tools for development and countries need to better understand the misuse of the emerging technologies.

DAY 2: Stocktaking the GFCE Supply Side

Asia-Pacific: What is your Recipe for Good CCB?

In the last few years, the Asia-Pacific region has seen new permanent structures for cyber capacity building being formed. Also, existing training, education and community organisations have embraced cyber as a new area of work. As global CCB efforts transition from project-driven to a more programmatic approach, it is important that CCB initiatives consider their effects on existing, new and emerging locally and regionally owned capability building structures.

In this session, representatives gave an overview of key regional initiatives for cyber capacity building and explained their recipes for good CCB in Asia and in the South Pacific. Speakers included ***Klée Aiken*** of CERT NZ, ***SeungJin Choi*** of the Republic of Korea Supreme Prosecutor's Office (KSPO) and ***Domingo Kabunare*** of the Kiribati ICT Policy and Development Division (MICTTD), who shared some lessons learned on how they have developed and refined their approaches to CCB. The session was moderated by ***Bart Hogeveen*** and ***Cherie Lagakali.***

One challenge mentioned by several speakers was contextualization. Often times CCB is being offered to individuals and communities with diverse backgrounds and varying levels of digital literacy. Targeting messages is very important when catering to different audiences. Dialogue with stakeholders and communities on how they digest what is being brought to them is crucial despite presenting specific challenges in itself. Talking directly with recipient communities helps in developing understanding of the impact that capacity building has and how it is received.

Another key aspect mentioned was the value of partnerships. Cooperation must be meaningful and built on consultation with key stakeholders if communities are to be empowered with accurate and useful knowledge on cybersecurity. Coordinated delivery needs to be consistent across the different target audiences and strong partnerships can help meet this objective.

Feedback is also very useful in getting campaigns across to communities. It helps if there is an open opportunity for people to ask questions about a campaign, as this enables a dialogue on the messages that are being transmitted and ensures that the campaign is accessible and well understood. Language is another key factor, as cultural differences can sometimes be a stumbling block. This is significant because language is the medium for knowledge transfer.

Some speakers took the view that coordination is a necessary component but not sufficient for making CCB impactful or sustainable. Making sure that the desired impact is actually being realized and amplifying this is usually more important than coordination. However, coordination can help with continuity where the efforts of those but with limited time or capacity can be taken up by others. This is particularly important for cyber capacity building as it should be long-term and cannot be done by one or two workshops or a single dialogue. It was reiterated that there is plenty of room for all actors – it is primarily important to ensure that efforts are being directed to all places where it is needed and that actors don't concentrate their efforts on just one thing. This is especially true when working with countries that are further behind in digital development as there are many things that still need to be done to achieve higher levels of cybersecurity capacity.

Stocktaking the GFCE Supply Side

The GFCE has evolved significantly since its establishment in 2015. Since then, an eco-system has been established to support international collaboration on cyber capacity building, tailor-made to the needs of the community. In this session, ***David van Duren***, GFCE Secretariat Director, assessed how the GFCE has progressed, with a specific focus on its supply side regarding cyber capacity content.

David began the presentation by underlining that the GFCE's mandate is to strengthen international collaboration and coordination on cyber capacity building. This is supported by two key elements that makes this platform unique: firstly, the GFCE is a member driven community which means that inclusion of members and partners or consultation is important; secondly, the GFCE is a neutral platform which is crucial for its coordinating role. The GFCE has gained a strong foundation on the supply side of capacity building through the accumulation of best practices, expertise and resources over the years. From 2015 until 2017, the GFCE focused on awareness raising and sharing expertise within the community. In the years 2018-2019 the GFCE set up tools (such as Cybil) and structures (such as the Working Groups) to support implementation of efforts. From 2019 to 2021, the GFCE ecosystem has been extended to deepen the way we work with the community, for example by establishing the Cybil Steering Committee, the Research Agenda and Research Committee; Regional Liaisons; and the Women in CCB Network.

Moving forward, there are several ways in which the GFCE will continue to build its supply-side of resources and expertise. Firstly, the GFCE will need to improve its tools with help from the whole community, supported by the GFCE Secretariat and Foundation Board. Immense value will be added by connecting the tools in suitable ways, such as linking the Clearing House with the Working Groups who are they key to connecting with the wider GFCE structures. Secondly, strengthening GFCE regional efforts through establishing regional hubs can strengthen regional CCB networks and empower the identification of local and regional needs. Thirdly, the GFCE will continue to initiate programs that activate and strengthen the eco-system. This means that regional projects will become more prominent as they enable scoping and implementation to be completed on a local level. Moreover, the Clearing House, as the GFCE's match-making function, is expected to grow. David stressed that if the GFCE Foundation or GFCE Secretariat are involved in these projects, their role is solely to coordinate, including bringing stakeholders together and identifying needs. This is the foundation that enables the GFCE community to deliver implementation activities.

Collaborating on CCB - What do the GFCE Working Groups have to Offer?

Established in 2018, the GFCE Working Groups provide a dedicated space for GFCE Members and Partners to meet and discuss specific topics, to collaborate, share knowledge, coordinate activities and network. In this panel, the Working Group Chairs reflected on the added value of the GFCE Working Groups and explored opportunities for the groups to reach those that are in need of more CCB support. The session was moderated by ***Richard Harris,*** with panelists ***Ian Wallace***, ***Abdul-Hakeem Ajijola***, ***Joyce Hakmeh***, and ***Tereza Horejsova***.

As highlighted by the Chairs, the GFCE Working Groups provide a unique opportunity to bring together various stakeholders from the multistakeholder community. Working with a bottom-up driven

approach, members & partners shape the working group's priorities every year, collaborate on initiatives based on similar interests on cyber capacity building, share experiences and expertise to avoid duplication of efforts, network with other stakeholders, and come together via online and physical meetings to discuss latest trends and developments on CCB.

One of the challenges mentioned during the panel discussion, is the need to make sure that the Working Groups' processes can help those who are in need for building and strengthening their cyber capacities. Although the groups are composed of a variety of stakeholders such as state actors, private sector, civil society, tech community globally, it is important to engage participation from regional and local actors who can benefit from the knowledge sharing and expertise on the global level. Another point brought up by the Working Group Chairs is how can the Working Groups promote the human-centric approach on cyber capacity building. As highlighted, human factor is in the center of creating and implementing policies and strategies on cyber capacity building; the Working Groups can thus help bringing together international and regional perspectives on this matter and make sure that institutions work towards more human-centric policies on cyber security.

The Chairs pointed out that the Working Groups are a cornerstone of the GFCE and a platform to share ideas, learn from each other and coordinate efforts. As the GFCE moves towards a demand-driven approach on CCB, it is crucial that full participation in the groups is encouraged to ensure that the needs of the global and regional multistakeholder players are being heard and that actions can be taken appropriately.

Refining the GFCE's Knowledge-Sharing Tools

Geared towards the needs of the GFCE community, the GFCE has developed tools to address and promote the sharing of knowledge and expertise which are the Cybil Knowledge Portal, the Clearing House and the Research Agenda. During this panel discussion, moderated by ***Carolin Weisser Harris*** from GCSCC, representatives from the GFCE tools, highlighted their benefits for the GFCE and wider CCB Community, and explored ways to ensure the tools evolve.

The chair of the Cybil Steering Committee, ***Stephanie Borg Psaila*** presented Cybil Knowledge Portal, an online repository that includes a wide range of resources, tools, projects related to cyber security and capacity building. Cybil is a unique tool, a one-stop portal that supports the GFCE's objectives of making expertise and information widely available by sharing tools, publication, projects, events, and best practices.

Next on the GFCE tools, ***Andrea Calderaro*** talked about the Global Cyber Capacity Building Research Agenda, a mechanism created to identify knowledge gaps and fill them with research. Supported by the GFCE Research Committee, the agenda helps expand our understanding on cyber topics, supports the development of projects and empowers the sharing of knowledge and expertise within the GFCE and the wider CCB community.

The Clearing House, presented by ***Manon van Tienhoven***, is the match-making tool of the GFCE. It is global mechanism that aims to connect countries' cyber capacity building needs with those who can offer support. Each clearing house case is unique and addressed with a tailored approach. With an effective clearing house mechanism, the GFCE aims to improve efficiency in the delivery of capacity building projects.

A new tool, the Knowledge Modules (KMs) was presented by ***Dr. Martin Koyabe***. The KMs, which are one of the outcomes of the AU-GFCE project, are going to be tailored made based on five thematic focus areas identified in the Delhi Communique, and will enable African countries to better understand and resolve their CCB needs. For their development, available CCB resources and tools will be extracted by Cybil, supplemented by input from regional and global experts. With the involvement of cyber experts within and outside the GFCE Community, the KMs follow a bottom-up driven approach based on local context that can be brought to the global level.

As mentioned by all panelists, these GFCE tools have an important and actual impact for the wider cyber capacity building community. It is crucial that we keep on raising awareness of the use the tools, by focusing on their success stories and their benefits on empowering knowledge and expertise sharing.

DAY 3: Bridging Demand and Supply for Cyber Capacity Building

Reflecting on Trends and Developments in Cyber Capacity Building

This session reflected on the trends and developments in cyber capacity building, and the ambitions for the GFCE for the coming year and how these fit into the identified trends. This session discussed the findings of the report "International Cyber Capacity Building: Global Trends and Scenarios," written by Robert Collett and Nayia Barmpaliou.

Robert Collett, Researcher and Project Consultant on International Cybersecurity Capacity Building, began the session highlighting that the report identified four trends in cyber capacity building (CCB). Firstly, the field of CCB is growing to include more actors that are increasingly interwoven. Secondly, aspirations for coordination have risen but implementation lags behind. Thirdly, more communities of practice are using CCB. Lastly, CCB is becoming increasingly professionalized.

In response to these trends, Robert provided recommendations addressed to the broad international CCB community and the GFCE as the leading international platform for CCB coordination and knowledge sharing. It is recommended that the CCB community prepares for the growth of the CCB field by adopting approaches that can scale, in addition to setting ambitious goals. Alongside this, the field should better bridge itself with parent communities such as the development community. In order to attract investment, the field should build and enhance its evidence base through research and published evaluations. CCB activity should also be better coordinated through enhanced internal information sharing such as through the GFCE or the Cybil Knowledge Portal. This should occur hand-in-hand with the professionalization of the field that calls for hiring specialist staff and training teams.

David van Duren, GFCE Secretariat Director, highlighted that the GFCE recognizes the four trends from the report, and has witnessed how CCB has grown to include more donors, recipients and implementing organizations. This growth is reflected in the GFCE's expansion from 42 members and partners during its establishment in 2015 to over 150 in 2022. He echoed the need for coordination, pointing out that this is why the GFCE was established six years ago, and called for more investments to be made in

coordination efforts. David pointed out that an additional trend he sees in CCB is the move towards a demand-driven approach in which countries and regions are more capable of defining their needs. A great example is the Africa CCB Committee, set up by the African Union and the GFCE consisting of all relevant African cyber capacity building organizations, including the 8 regional organizations. The committee will define new CCB projects based on African needs and support implementation efforts. The GFCE Secretariat will liaise with the committee to bridge it to the GFCE community.

With regards to recommendations of report, David agreed that as the need for CCB grows, efforts need to be scaled up. As part of this, the GFCE Clearing House, being the GFCE's match-making function, is expected to grow in use in the near future. Regarding the need to build an evidence base for investment, he hopes the GFCE can make use of research done by the GFCE community such as through the GFCE Research Agenda. Moreover, to improve coordination and knowledge sharing, he explained that the GFCE aims to scale up and receive more support for coordination through setting up regional hubs, or setting up coordination networks. On the need to bridge the divide between CCB communities and parent communities, the GFCE requires support from the GFCE community to take steps towards this through voicing commitment and providing resources. On the whole, as the CCB field evolves, the GFCE will mature and adapt to these developments.

Raising the Stakes in Cyber Capacity Building

Cyber capacity building is maturing as a concept and the GFCE has a role in raising the stakes and position cyber capacity building higher on the international agenda. This panel, moderated by ***Francesca Bosco*** from CPI, addressed the main developments and opportunities for achieving this.

Nick Natale, Global Affairs Canada, highlighted that the GFCE is a great place to conduct a lot of coordination and engagement tasks that the OEWG needs. This is in response to the fact that the UN is creating a new body to coordinate CCB, which Canada believes to be a duplication of existing efforts by the GFCE. Thus, Nick stressed that the community needs to come together to position the GFCE to the OEWG as a platform that already has the capacity to consolidate requests for needs (such as through the GFCE Clearing House) and the ability to coordinate tailored projects to ensure projects align with objectives of OEWG.

Francesca Spidalieri, Hathaway Global Strategies, referred back to the Integrating Cyber Capacity into the Digital Development Agenda Report, commissioned by the GFCE, as a practical example of how the GFCE is positioning CCB higher on an international agenda and how it is connecting the CCB community with the broader development community. Francesca also underlined that the GFCE has an opportunity to build a coalition of champions to convince the OECD committee to add digital resilience as part of the criteria. Moreover, she stressed that the GFCE should continue to expand its platform by bringing in more organizations and expanding its Clearing House function.

Mark Williams, World Bank, highlighted that the World Bank's partnership with GFCE has been essential and is critical to the CCB landscape. Mark echoes Francesca's calls to integrate CCB with the development community, highlighting that cooperation between the two fields has been vastly beneficial so far. He stressed that the Cybil Portal is another example of how the GFCE enhances knowledge-sharing and thus the World Bank supports the deepening and broadening of the portal. Moreover, in order to ensure high-level attention to CCB issues, the World Bank is looking forward to hosting the Global Conference on Cyber Capacity Building (GCCCB) in Washington in autumn of 2022.

Chris Painter, President of the GFCE Foundation Board, expressed that the timing is right, due to the ongoing UN processes and ransomware becoming a mainstream issue, to raise CCB as a political priority issue. He agrees with Francesca that a key way forward is mainstreaming CCB within the development agenda and bridging with the development community. A key enabler for success is the inaugural GCCCB that will take place in the third quarter of 2022. Chris underlined that the key desired outcomes would be to have a joint international declaration for CCB, and hopefully going one step further by turning this into a program with funding. Additionally, another key outcome would be to foster multi-stakeholder cooperation, particularly by promoting public-private partnerships.

Multistakeholder Reflections on the Way Forward for Cyber Capacity Building

As the GFCE is a multistakeholder global platform on cyber capacity building, this session, moderated by ***Nils Berglund*** from EUISS, focused on a dialogue between different stakeholder and their views on the way forward for CCB.

Nikolas Ott, representing Microsoft, started the discussion by reflecting on the GFCE's role in the broader multi-stakeholder cyber ecosystem. It is important that multistakeholder communities like the GFCE prove their added value by facilitating information sharing and enabling output-oriented work as this can help ensure engagement from a multitude of actors. The GFCE stands out as a center of coordination and as a platform for information-sharing. There are a lot of examples of how societies benefit from the GFCE as an enabler of multi-stakeholder collaboration. However, we need to be more proactive as a community in bringing practical and technical knowledge and expertise to those in need in order to develop awareness and skills.

No individual or stakeholder group can do this alone. ***Daniela Schnidrig***, representing Global Partners Digital, reiterated that civil society helps foster a cyberspace that is underpinned by human rights, transparency and accountability, adding a depth of knowledge to collaborative cyber capacity building. Civil society also plays a strong role in the evaluation of policy and strategy, ensuring that policy is evidence-based, helping to track government engagement and adherence to international norms and push for norms implementation through national frameworks. We need to focus our engagements on excluded groups, to demystify cyber security and its framings to make it more approachable for everyone and step out of the narrow understanding of CCB.

Elina Noor, representing the Asia Society Policy Institute, considered that the cyber capacity building needs to be multistakeholder but also cross-sectoral. A focus on a demand-driven approach indicates that the community is listening to the priorities of countries in need of cyber capacity building. However, what happens at the international level must be translated to regional, national and local community contexts. In ASEAN we are witnessing cross-cutting efforts to implement norms for responsible state behavior agreed at the multilateral level through institutions and mechanisms in response to cyber challenges.

At the policy level, high-over discussions about cyberspace at international level differ from national and local level, where efforts are focused on leveraging the power of digital technology to effectively advance the development agenda and economic priorities. The international context needs to be more inclusive of varying views and approaches as the past two years have made our divergences in terms of capacity more acute. We also need to enable innovative thinking that takes account of differing ways of transferring knowledge across communities as this will affect how CCB can influence and bring change

and social justice to societies.

Platforms such as the GFCE Working Groups and Research Agenda deserve special mention as they are strong examples of a community-driven approach which provide opportunities for all stakeholders to engage with each other, submit their own ideas and push for funding, which is often a missing aspect. Other efforts, such as an initiative the GFCE Advisory Board is developing to engage further with civil society also go towards these objectives. The High-Level Conference planned for next year is a good opportunity to bring stakeholders across different sectors together and raise awareness about smaller communities with less resources.

Ultimately there is no silver bullet and building these bridges is a responsibility of all in the GFCE community. Approaches to cyber capacity building need to be holistic to help attract distanced communities and broaden our understandings. Increased investment needs to be complimented with better coordination and a two-way framework for sharing knowledge and expertise whilst ensuring needs are met.

Closing Ceremony

Chris Painter, President of the GFCE Foundation Board, closed the GFCE Annual V-Meeting 2021 by providing a few closing remarks. He summarized that, moving forward in 2022, the GFCE is focusing on evolving the GFCE community and its ecosystem which calls for a three-fold approach. Firstly, tailoring supply by moving to a demand-driven approach. Secondly, strengthening regional coordination to bridge the national and global level. And thirdly, maturing to an integrated GFCE ecosystem. He highlighted that this Annual V-Meeting has been instrumental in getting the GFCE closer to these aims. In particular, the community has discussed how the GFCE can move towards a demand-driven approach with the objective to tailor supply to demand through coordinating local scoping exercises regionally and further integrating the GFCE ecosystem. Looking ahead, the GFCE is eager to implement these insights to ensure our steps forward reflect the needs of the community.

GFCE Deliverables presented at the Annual V-Meeting 2021

GFCE Report "Integrating Cyber Capacity into the Digital Development Agenda"

Written by Melissa Hathaway and Francesca Spidalieri, the report identifies pathways to bridge the development community to the cybersecurity capacity building community. The report describes some of the key challenges and benefits of incorporating cybersecurity & capacity building into the development agenda.

EUISS Report "International Cyber Capacity Building: Global Trends and Scenarios"

Written by Robert Collett and Nayia Barmpaliou and funded by the EU, the report identifies the latest trends in cyber capacity building and proposes potential scenarios for the cyber capacity building field.

Global Cyber Capacity Building Research Agenda 2022-2023

The aim of the Research Agenda is to help the capacity building community design and run more effective projects by identifying knowledge gaps & filling gaps through research. The GFCE Community identified 24 cyber knowledge gaps and highlighted 7 of them as having high priority.

Global Cyber Expertise Magazine

The 10th issue of Global Cyber Expertise Magazine covers a range of topics on cybersecurity, with articles about the latest developments on CCB from each of the four regions (Europe, Asia & Pacific, Americas and Africa), such as the AU-GFCE collaboration project, the ASEAN- Japan Cybersecurity Capacity Building Centre and the European Cyber Agora.

GFCE Working Groups Annual Report 2021

The Working Groups identified three general objectives for 2022:

- Knowledge and expertise sharing through regular engagement opportunities
- Support contributions to and use of the GFCE tools
- Provide a platform for GFCE members and partners to showcase expertise

Cybil Annual Report 2021

The Cybil Portal is an online repository for international cyber capacity building projects and hosts a large library of resources for projects to use. 2021 was a year of growth for the Portal: unique monthly users doubled to over 3000; it gained new features, such as an events calendar and recordings of webinars; and its content grew by 160 projects and 61 resources.

Program & Speakers Overview

Opening GFCE Meeting & Strategic Way Forward
Tuesday 30 November, 13:00-13:30 UTC

Christopher Painter
President of the Foundation Board, Global Forum on Cyber Expertise

Maartje Peters
GFCE co-Chair & Head of Taskforce International Cyber Policy of the Ministry of Foreign Affairs of the Netherlands

Ajay Prakash Sawhney
GFCE co-Chair, Secretary at the Ministry of Electronics and Information Technology of India

Joanna Kulesza
GFCE Advisory Board co-Chair, Assistant Professor at the University of Lodz

Marjo Baayen
Director of the GFCE Secretariat

Regional Cyber Capacity Building Priorities
Tuesday 30 November, 13:30-14:15 UTC

Folake Olagunju
GFCE Advisory Board co-Chair, Program Officer of Internet and Cybersecurity, ECOWAS

Manon Le Blanc
Head of the Cyber Sector at the EU Diplomatic Service, European External Action Service (EEAS)

Ka Man Yip
Head of Capacity Building Desk International Cyber Police Office, Cyber Security Agency of Singapore

Kerry-Ann Barrett
Cyber Security Policy Specialist (OAS), GFCE-OAS Liaison Officer

Dr. Towela Nyirenda-Jere
Planning and Coordinating Agency Programme Officer at AUDA-NEPAD

Cherie Lagakali
GFCE Pacific Liaison Officer

Strengthening the demand-driven approach in Africa
Tuesday 30 November, 14:25-14:55 UTC

Dr. Towela Nyirenda-Jere
NEPAD Planning and Coordinating Agency Programme Officer

Dr. Martin Koyabe
Senior Project Manager for the African Union - GFCE Collaboration Project

Abdul-Hakeem Ajijola
Chair African Union Cyber Security Expert Group & Chair GFCE Working Group B CIM and CIIP

Integrating Cyber Capacity to the Digital Development Agenda
Tuesday 30 November, 14:55-15:55 UTC

Melisa Hathaway
President of Hathaway Global Strategies LLC
David Satola
Lead ICT Counsel World Bank
Vladimir Radunovic
Director, E-diplomacy and Cybersecurity Programmes at DiploFoundation
Kerry-Ann Barrett
Cyber Security Policy Specialist (OAS), GFCE-OAS Liaison Officer
Kanwaljit Singh
Senior Program Officer, Bill & Melinda Gates Foundation
Patryk Pawlak
Brussels Executive Officer at EUISS

Asia-Pacific: Recipes for Good CCB
Wednesday 1 December, 03:00-04:30 UTC

Klée Aiken
Principal Advisor at CERT NZ
Domingo Kabunare
Senior Information Security Analyst, Kiribati
Choi SeungJin
Republic of Korea
Cherie Lagakali
GFCE Pacific Liaison Officer
Bart Hogeveen
Head of Cyber Capacity Building at ASPI

Stocktaking the GFCE Supply Side
Wednesday 1 December, 13:00-13:20 UTC

David Van Duren
Director of the GFCE Secretariat

Collaborating on CCB – What do the GFCE Working Groups have to Offer?
Wednesday 1 December, 13:25-14:05 UTC

Richard Harris
Principal Cybersecurity Policy Engineer at MITRE Corporation, GFCE Advisory Board Member & Research Committee Member

Ian Wallace
Senior Adviser for Cybersecurity Policy, Office of the Coordinator for Cyber Issues, U.S. Department of State, Chair of GFCE Working Group on Cyber Security Policy & Strategy

Abdul-Hakeem Ajijola
Chair of the African Union Cyber Security Expert Group and Chair of GFCE Working Group B on Cyber Incident Management & Critical Information Protection

Joyce Hakmeh
Senior Research Fellow at Chatham House, Chair of GFCE Working Group C on Cybercrime

Tereza Horejsova
Director or Project Development and Partnerships in DiploFoundation, Chair of GFCE Working Group D on Cyber Security Culture & Skills

Refining the GFCE's Knowledge-Sharing Tools
Wednesday 1 December, 14:15-15:00 UTC

Carolin Weisser Harris
Lead International Operations, Global Cyber Security Capacity Centre (GCSCC), GFCE Task Force Strategy & Assessments co-Lead and Cybil Steering Committee Member

Dr. Martin Koyabe
Senior Project Manager for the African Union - GFCE Collaboration Project

Stephanie Borg Psaila
Director for Digital Policy at Diplo Foundation, Cybil Steering Committee Chair

Andrea Calderaro
Associate Professor at Cardiff University, GFCE Research Committee Member

Manon van Tienhoven
Program Coordinator GFCE Secretariat

Reflecting on the Trends & developments in Cyber Capacity Building
Thursday 2 December, 13:00-13:30 UTC

David Van Duren
Director of the GFCE Secretariat

Robert Collett
Researcher and Project Consultant on international Cybersecurity Capacity Building

Raising the Stakes in Cyber Capacity Building
Thursday 2 December, 13:30-14:15 UTC

Mark Williams
Practice Manager, Global Knowledge and Expertise for the Digital Development global practice at World Bank
Francesca Spidalieri
Cybersecurity Consultant, Hathaway Global Strategies LLC
Francesca Bosco
Chief of Staff, Head of Foresight at The CyberPeace Institute
Nicholas Natale
Senior Project Manager for Global Affairs Canada
Christopher Painter
President of the Foundation Board, Global Forum on Cyber Expertise

Multistakeholder Reflections on Way Forward for Cyber Capacity Building
Thursday 2 December, 14:25-15:10 UTC

Nils Berglund
Outreach and Public Engagement Coordinator for the EU Institute for Security Studies
Nikolas Ott
Cyber Project Manager for Microsoft, GFCE WG A Task Force co-lead CBMs, norms & cyberdiplomacy
Daniela Schnidrig
Senior Program Lead, Global Partners Digital & GFCE Advisory Board Member
Elina Noor
Director, Political-Security Affairs & Deputy Director, Washington D.C. Office, Asia Society Policy Institute, Cybil Steering Committee Member

Closing Ceremony
Thursday 2 December, 15:10-15:25 UTC

Christopher Painter
President of the Foundation Board, Global Forum on Cyber Expertise