GFCE ANNUAL MEETING 2020 | REPORT

GLOBAL FORUM ON CYBER EXPERTISE

Report on the GFCE Annual Meeting 2020

Coordinating a Global Network on Cyber Capacity Building

Objective of the GFCE Annual Meeting 2020

The focus of the GFCE in 2020 was on consolidating its position as the coordinating platform for cyber capacity building and further strengthen international collaboration and expertise globally. To achieve this, the GFCE has focused on the following long-term goals:

i. Coordination: Avoid duplication and fragmentation of CCB efforts globally by supporting coordination activities;

ii. Knowledge sharing: Make relevant CCB knowledge and expertise available on a global scale (e.g. through the Cybil Knowledge Portal);

iii. Matchmaking: Match requests of cyber capacity needs from GFCE members with offers of support;

iv. Collaboration: Cooperating on new projects within the GFCE community

This year is a special milestone for the GFCE as it celebrated its fifth (5th) anniversary in April 2020. During these five years, the GFCE has managed to achieve concrete deliverables, has an engaged GFCE community, has gained a strong online presence, and has grown from 42 initial founding members to an organization with over 120 members and partners from all regions of the world. Committed to its mission strengthen cyber capacity building globally, the GFCE Annual V-Meeting on 24 & 25 November was focused on sharing the GFCE outcomes of 2020 and present the Work Plan and ambitions for 2021. The Annual V-Meeting was built on the GFCE Strategic Building Blocks formulated by the GFCE Foundation Board, six (6) fundamental blocks guide the directions to the GFCE and its community for 2020 – 2021.

The GFCE Strategic Building Blocks are:

Image 1: GFCE Strategic Building Blocks 2020 – 2021

With the global changes happening due to the COVID-19 pandemic, this year the GFCE hosted its ever first virtual Annual Meeting, by using on online experience platform. This GFCE virtual platform created an online venue where all GFCE Members and Partners can come together to attend sessions, showcase deliverables, and have bilateral conversations in order to make steps to improve global cyber capacity building. During the two-day virtual meeting, the platform brough together more than 200

representatives from governments, NGOs, international organizations, academic and tech communities and civil society. In this report, you will find an overview of the GFCE Deliverables 2020, a short summary of the sessions during the Annual V-Meeting together with outcomes and next steps for 2021.

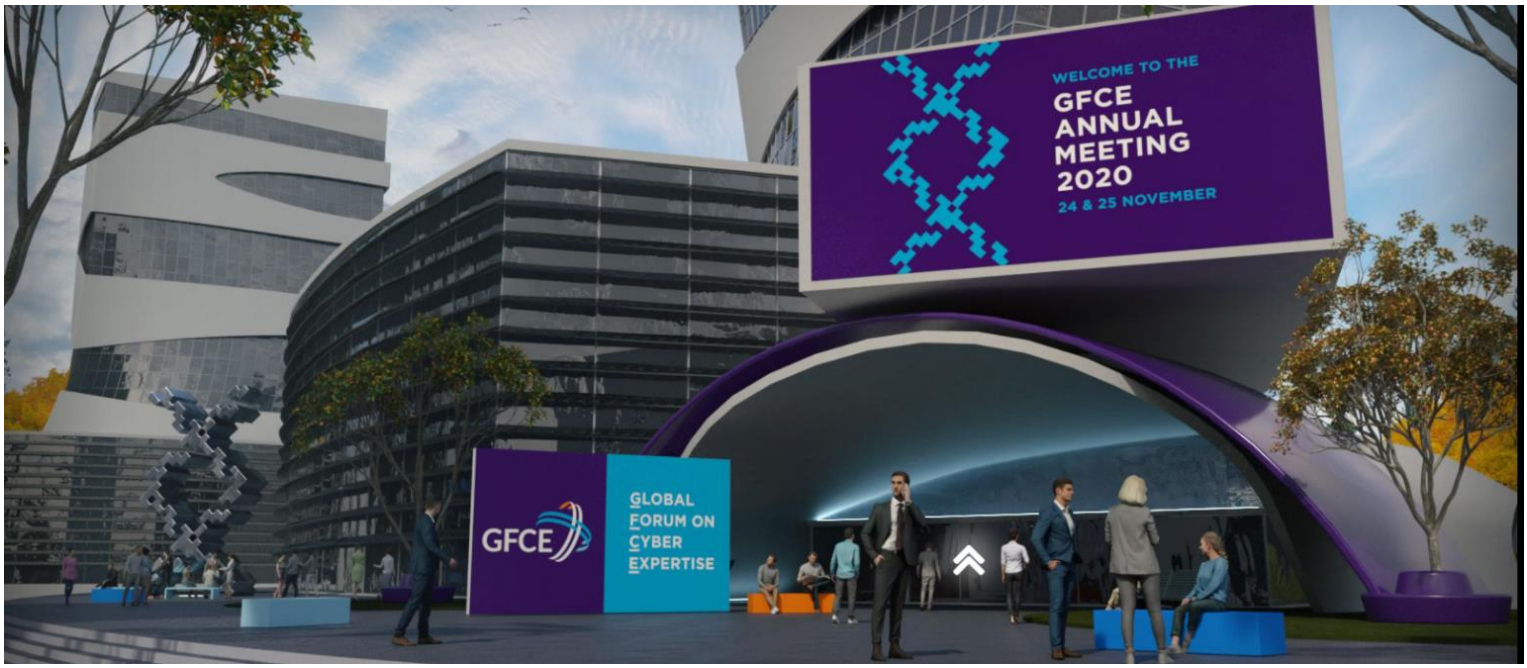

Image 2: GFCE Annual V-Meeting Virtual Platform Entrance

GFCE Achievements 2020

Despite the challenges brought to all organizations by the global COVID-19 pandemic in 2020, the GFCE accomplished to set and achieve concrete deliverables within the GFCE Working Groups, focused on setting the first Global Cyber Capacity Building Research Agenda, collaborated on GFCE initiatives with other stakeholders, set up regional meetings, participated in online conferences and initiated new projects. Kindly see below an overview of the GFCE deliverables 2020:

- The establishment of the **GFCE Foundation Board** in January 2020, to support and strengthen the GFCE efforts;
- The GFCE 5th Anniversary in April with the implementation of the **GFCE V-Meeting series** of a 7-week online webinars;
- The introduction of the new GFCE tool the **Global Cyber Capacity Building Research Agenda,** with **fifteen (15) research ideas identified** to help design and run projects by identifying knowledge gaps and filling gaps through research;
- The introduction of the six (6) **GFCE Strategic Building Blocks** to guide the directions of the GFCE in 2021;
- The establishment of the **GFCE Research Committee**, to provide Working Groups with expert assistance to translate ideas into research questions with time/cost estimates and delivery requirements;
- The appointment of the **GFCE Working Groups Chairs 2020 – 2022**, responsible for monitoring the overall work plan of the Working Groups and activating the members towards opportunities for collaboration;
- The appointment of the **GFCE Advisory Board 2020 – 2022,** to provide advice on the overall strategic direction of the GFCE to ensure that cyber capacity building activities under the GFCE umbrella reflect the multi-stakeholder approach to policy making;
- The updated **GFCE Clearing House Mechanism**, connecting cyber capacity needs and offers for support;
- The **GFCE Regional Meetings** in Europe (January 2020) and Melbourne (February 2020);
- The establishment of the **GFCE Women in CCB Network** to connect female experts in CCB and facilitate the implementation of projects;
- The scope of a future **GFCE Pacific Hub,** to facilitate national and regional cyber capacity building coordination and information sharing;
- The launch of the new **GFCE Website**, with updated information on the work of the GFCE;
- The **GFCE Working Groups'** deliverables for 2020 and their Work Plan for 2021;
- The achievements of **Cybil Knowledge Portal** during 2020 with more than 500 actors, 600 projects, 100 publications and 1000 visitors a month;
- The **GFCE collaboration with the Gates Foundation and the African Union** to deliver CCB training modules and identify a number of key CCB challenges in Africa.

GFCE Annual V-Meeting 2020 Program

Below you can see an overview of the two-day program with links to watch the sessions. On the following pages you will find a short summary of all sessions.

TUESDAY 24 November - DAY 1	
Time (UTC)	**Session**
13:00 – 14:00	Opening Ceremony
14:10 – 15:10	Challenges to Cyber Capacity Building in the (Post-) COVID-19 Era
16:15 – 17:00	Empowering the GFCE Women in CCB Network
16:15 – 17:00	Outcomes of GFCE Regional Meetings 2020

WEDNESDAY 25 November - DAY 2	
Time (UTC)	**Session**
06:00 – 08:00	Coordinated ICT and Cyber Capacity Building in the Pacific
13:00 – 14:00	GFCE Toolbox: Research Agenda, Cybil Portal & GFCE Clearing House
14:10 – 14:55	GFCE as a Platform for Multi-Stakeholder Cooperation
14:10 – 14:55	Supporting National & Regional Cyber Capacity Needs in Africa
15:05 – 15:50	GFCE in the Spotlight: How to strengthen the GFCE brand in the global CCB arena
15:05 – 15:50	Accelerating the adoption of Open Internet Standards
16:00 – 17:00	Exploring a High-Level CCB Conference in 2021
17:00 – 17:15	Closing Ceremony

DAY 1

Tuesday 24 November 2020

The first day of the GFCE Annual V-Meeting focused on the following GFCE Strategic Building Blocks: Make the GFCE community more inclusive; Enhance collaboration in the GFCE community; and Increase the GFCE's regional focus.

The Annual Meeting officially started with the Opening Ceremony by: Ajay Prakash Sawhney & Carmen Gonsalves (GFCE co-Chairs), Christopher Painter (GFCE Foundation Board President), Folake Olagunju & Joanna Kulesza (GFCE Advisory Board co-Chairs), announcements by the GFCE Community and the presentation of the GFCE Work Plan 2021 by David van Duren and Marjo Baayen (GFCE Directors).

Challenges to Cyber Capacity Building in the (Post-) COVID-19 Era

Moderator: **Alison Treppel** (Organization of American States)
Speakers: **Ian Wallace** (GFCE Working Group A Chair/ German Marshall Fund), **Abdul-Hakeem Ajijola** (GFCE WG B Chair/Chair of the AUCSEG), **Joyce Hakmeh** (GFCE WG C Chair/Chatham House), **Tereza Horejsova** (GFCE WG D Chair/DiploFoundation), **Moctar Yedaly** (African Union Commission).

The aim of the session was to discuss how the (post-) COVID-19 has affected and changed Cyber Capacity Building (CCB) globally; what type of challenges have arisen in 2020 due to the global pandemic's consequences and how these challenges have impacted on the CCB landscape. The panel, moderated by Alison Treppel, pointed out the opportunity brought from COVID-19 to put things into perspective and understand how much technology has affected people's daily working lives. Technology has managed to replace the physical presence of people at the office, in conferences and has brought more flexibility than before. With the technological advances coming due to COVID-19, one thing is more important than ever: to understand that CCB plays a crucial role in the online environment and should remain high on the cyber security agenda.

Empowering the GFCE Women in Cyber Capacity Building Network

Moderator: **Kerry-Ann Barrett** (Organization of American States)
Speakers: **Carmen Gonsalves** (GFCE co-Chair/The Netherlands), **Bonnie Butlin** (Security Partners' Forum, Canada), **Szilvia Tóth** (OSCE), **Katherine Getao** (ICT Authority, Kenya).

The aim of the session was to bring the GFCE Women in CCB Network together and discuss opportunities for collaboration under the GFCE umbrella. The focus was given on highlighting the added value of the GFCE Network and the importance of connecting women from different working backgrounds to collaborate on cyber capacity building efforts.

In the beginning of the session, several female experts in the field of cyber security shared their view on why it is important for women to collaborate on cyber capacity building. Women can bring innovation to the field, can empower each other, bring dynamic and wealth of experience and can influence young girls through training opportunities in the field of cybersecurity. The panelists pointed out that the GFCE Network provides a unique opportunity for women from all over the world to come together, reach out to each other, align views and exchange ideas, but most of all inspire young women generations and collaborate on projects to shape the field of cyber security. In addition, the GFCE Network can connect

to other global and regional networks in order to ensure that regional female needs are also represented and covered. One of the opportunities for collaboration pointed out by the panelists, is the development of education and skill trainings in order to empower young professionals to follow cyber security career paths and reach leadership positions. To do this, in 2021, the GFCE should try to reach out to potential organizations that have a business culture which empowers gender inclusivity and support mentorship and training programs.

Outcomes of GFCE Regional Meetings 2020

Moderator: **Louise-Marie Hurel** (GFCE Advisory Board)
Speakers: **Cherie Lagakali** (GFCE Pacific Liaison), **Robert Collett** (EUISS).

The aim of the session was to summarize the GFCE's approach to outreach and engagement, hearing about the outcomes of the GFCE's regional Pacific meeting (February 2020) and EUISS's project to map global CCB trends.

Regarding the Pacific region, one of the key outcomes of the meeting in February was the design and creation of a future GFCE Pacific Hub, now led by Cherie Lagakali, GFCE Pacific Liaison. Cherie explained that the Pacific region continues to face several challenges such as the need of proper Cyber Capacity Building (CCB) facilitation and coordination between donors and implementers and avoiding the duplication of efforts and the wasting of resources and time. A future GFCE Pacific Hub aims to establish sustainable relationships with all donor and implementer actors in the region, while building sustainable, political support with the Pacific Island Nations and other regional organizations to prioritize CCB support. The success and primary objectives of a GFCE Pacific Hub will be to ensure it is about the Pacific and for the Pacific.

Robert Collett proceeded to present EUISS's and GFCE's joint research project examining trends in Cyber Capacity Building using heavily the information contained on the **Cybil Knowledge Portal.** The research aims to provide EU staff with operational guidance on CCB, while also informing the international community on global CCB trends. Robert explained that research conducted thus far has led to a framework for categorizing trends being agreed: Thematic, Regional and Programmatic.

i. Thematic: as the complexity of international CCB projects increases, new project areas have emerged such as gender, inclusion and responses to COVID-19', which cut across traditional CCB subjects
ii. Regional: although CCB has spread globally, there are clearly concentrations of CCB projects in some regions and examples of countries receiving no direct support
iii. Programmatic: there is a drive to professionalize CCB with the emergence of multi-million, multi-year programs adopting many of the methods of the developing community. Driving these programs is a need for better measurement and the communication of CCB success and impact.

DAY 2

Wednesday 25 November 2020

The second day of the GFCE Annual V-Meeting 2020 focused on the following GFCE Strategic Building Blocks: Strengthening the GFCE Brand; Enhance collaboration with the GFCE community; Connect with other platforms and processes; and Enlarge the pool of international resources. Kindly see below a brief overview of the sessions.

Coordinating ICT and Cyber Capacity Building in the Pacific Region

Speakers: Hon. Simon Kofe (Minister of Justice Communications and Foreign Affairs of Tuvalu), **Chris Painter** (GFCE Foundation Board), **Cherie Lagakali** (GFCE Pacific Liaison), **Bart Hogeveen** (ASPI), **Klée Aiken** (CERT NZ).

This session aimed to build engagement and momentum with the Pacific on CCB, following the GFCE's Regional Meeting in Melbourne (February 2020), and aimed to discuss the coordination, prioritization and sharing of expertise on thematic CCB and digital development subjects in the Pacific.

The session opened with remarks from Hon. Simon Kofe and Chris Painter on the evolving digital and CCB landscape in the Pacific. Both stressed the fact that as the global pandemic has accelerated the adoption of digital technologies in the Pacific region, the exposure and risk of the Pacific Island Nations becoming victims of cybercrime has increased. The risk of cybersecurity has been noted by the region's leader in part in the Boe Declaration. Pacific islands are aware that tackling cybercrime requires robust regulatory and legal apparatuses. CCB challenges in the region continue to revolve around coordination, local political commitment, and contextualized interventions. The panelists further added to these challenges the following: lack of cybersecurity skills and awareness, need to enact legal frameworks and regulations on privacy and cybercrime and lack of capacity to research regulatory and legal issues relating to digital access and economy.

Following these remarks, the session continued with three breakout rooms on the following subjects: e-safety and cybercrime, cybersecurity workforce skills and digital development and e-governance with the aim of discussing CCB activities, opportunities and challenges in the Pacific. The e-safety and cybercrime breakout highlighted that although the region is improving in prioritizing e-safety issues, there is still a difficulty in understanding what and how the Pacific can baseline cyber safety enabling the prioritization of the region's limited resources. The cybersecurity workforce and skills breakout discussed the supply (i.e. accessible material) and demand side (i.e. lack of jobs) challenges of building cybersecurity skills and agreed that accessibility, affordability and feasibility are all challenges that individuals face in upskilling themselves on cyber security training opportunities. The participants pointed out that a future GFCE Pacific Hub could help address cyber workforce and skills initiatives at local and regional levels. Lastly, the digital transformation and e-governance breakout agreed that digital connectivity, quality of access and affordability remain priorities. All agreed that future governance security standards would have to be tailored for the Pacific environment, recognizing the region's unique geographical landscape, user's base and connectivity.

GFCE Toolbox: Research Agenda, Cybil Portal & Clearing House

Moderator: **Joanna LaHaie** (USA)
Speakers: **Enrico Calandro** (GFCE Research Committee Chair/C3SA), **Ole Willers** (Cybil Steering Committee/NUPI), **Carolin Weisser-Harris** (GCSCC), **Manon van Tienhoven** (GFCE Secretariat).

This session aimed to promote greater understanding of the three GFCE tools that are available to both the GFCE and the broader cyber capacity building community: the Global CCB Research Agenda, Cybil – the CCB knowledge portal, and the GFCE Clearing House. An update was given on each of the tools including their current stage of development, and the value of the tools in supporting the practical implementation of CCB was underlined.

The **Global CCB Research Agenda** is a new tool developed for and by the GFCE Community to help the capacity building community design and run more effective projects by identifying knowledge gaps and filling gaps through research. The GFCE Working Groups and Task Forces, with the support of the **GFCE Research Committee**, were called to propose research ideas, and a total of fifteen (15) research ideas were identified for the draft Research Agenda. Over half of the GFCE Community participated in this first agenda-setting exercise to determine the prioritization of the research ideas. The draft Research Agenda and the prioritization list was shared during the session and can be found **here**. For 2021, the research ideas that are higher on the prioritization list will receive funding and become a research project.

Next, the **Cybil Knowledge Portal** launched in 2019, was re-introduced and its new features and plans for 2021 were shared with the participants. In September 2020, Cybil management was transferred to the GFCE Secretariat and in November, the Cybil Steering Committee was established to provide guidance, advice and views on Cybil. Over its one year of establishment, Cybil has been used by the community to share their reports/tools/publications, to search for project information and to look for upcoming events on cyber security. For 2021, Cybil will connect with other portals in order to avoid the duplication of information, include more visualization, create a new section for webinars, raise awareness, improve content and will recruit new members for the Cybil Steering Committee.

Lastly, the **Clearing House** is a GFCE tool aiming to improve efficiency in the delivery of CCB programs through coordination and increase knowledge sharing between stakeholders. The function of the Clearing House is to be the broker between capacity needs and offers for support, available to all GFCE members and partners. Additionally, as each cyber capacity building request is unique, each request is assessed on a case by case basis and a plan of action is determined based on the needs of each case. The Clearing House process has thus far helped Sierra Leone and Tunisia with their National Cyber Security Strategies, Senegal with a workshop on its Critical Infrastructure Protection and The Gambia with cybercrime legislation. In 2021, the GFCE aims to offer an effective and internationally recognized clearing house for cyber capacity building with a scalable process, a portfolio of expertise and a systematic gathering of project information with national and regional context.

Supporting National and Regional Cyber Capacity Needs in Africa

Moderator: **Daniela Schnidrig** (GFCE Advisory Board/Global Partners Digital)
Speakers: **Racky Seye** (Senegal), **Folake Olagunju** (GFCE Advisory Board co-Chair/ECOWAS), **Moctar Yedaly** (AUC).

This session focused on how the GFCE community can support national and regional cyber capacity building priorities in Africa, improving the future design, implementation, and coordination of CCB projects across the continent.

The panelists discussed the recently agreed partnership between the GFCE, Gates Foundation and the African Union to deliver CCB training modules and identify a number of key CCB challenges in Africa, ranging from a lack of cyber strategies, cyber legislation and assistance in building and facilitating CERT to CERT relationships. An important point raised is the need for current and future CCB activity in Africa to recognize diversity and importance of language, translating CCB learning and information into regional languages/dialects. The panel further highlighted the role the GFCE could play in helping African countries facilitate CCB activities, recognizing the localization of issues and the need to build trust and shared resilience. Cyber diplomacy, is also becoming an important subject of CCB in Africa, assisting and encouraging countries to engage with international cyber debates such as the UN OEWG. The panelists also pointed out that the GFCE Clearing House Function could serve as an effective, neutral platform to help match international CCB resources and expertise with African CCB needs. Racky Seye also shared Senegal's experience with the GFCE Clearing House mechanism, supporting the country's development of its National Cyber Security Strategy.

GFCE as a Platform for Multi-Stakeholder Cooperation

Moderator: **Francesca Bosco** (CyberPeace Institute)
Speakers: **Sithuraj Ponraj** (CSA Singapore), **Lea Kaspar** (Global Partners Digital), **Nthabiseng Pule** (C3SA), **Danielle Kriz** (Palo Alto Networks).

This session aimed to examine how the extensive knowledge and expertise within the GFCE could be leveraged to enable practical collaboration between stakeholder groups. Speakers were called upon to share their experiences on how multi-stakeholder approaches can be used to instill a greater sense of "ownership" of responsibilities and encourage commitments from various actors.

The panelists pointed out that although cyber capacity building requires collaboration that is cross-disciplinary and cross-regional, there is a fundamental need to understand what multi-stakeholder approaches mean in the context in which they are applied. In that sense, depending on the objective of the effort and on the resources available, different approaches to identifying relevant actors and engaging stakeholders will need to be employed. This was identified as a concept of "multi-stakeholder by design", which incorporates the need to have identified stakeholders involved in capacity building from the very beginning to ensure diversity of participants and to create a sense of ownership so that the initiative can be promoted and ensure its sustainability. Capacity building effort programs can seek to build knowledge using a modular approach, taking into account the differences in operational, technical and policy cooperation. This is linked to an understanding of the needs of recipients or beneficiaries, as well as the specific objectives of the program or project. As a champion of a multi-stakeholder approach to cyber capacity building, the GFCE can and should do more to promote the importance and value of multi-stakeholder approaches to CCB in different discussions taking place around the world. At the same time, the GFCE is itself a good example of multi-stakeholder cooperation

and should continue in its efforts to open up its network and platform to all stakeholders so that all can enjoy the benefits of coordination on cyber capacity building.

GFCE in the Spotlight: How to strengthen the GFCE brand in the global CCB arena

Moderator: **Richard Harris** (GFCE Advisory Board & Research Committee member/MITRE)

The objective of this session was to discuss with the GFCE community new ideas to promote externally the GFCE's brand and visibility and explore how the GFCE can expand its work and connect with other platforms/fora on Cyber Security and Capacity Building. The session was fully interactive using a Q&A tool, moderated by Richard Harris.

The participants of the session shared their views on the visibility of the GFCE Brand and how this can be strengthened online raising the following ideas: creating bilateral COMs relations with GFCE members & partners, create and participate in more online events and strengthen the GFCE's digital marketing. To support the GFCE brand visibility, participants also suggested that it is necessary for the various GFCE entities (i.e. Advisory Board, Foundation Board) to share the work of the GFCE with their own network, highlight key outcomes and deliverables more regularly, communicate the work of the GFCE in international conferences and forums. Additionally, another important point raised by the community was the need for the GFCE to expand its brand visibility regionally, especially in the Pacific and Africa region, by hosting meetings involving key regional stakeholders. Lastly, it was highlighted that the GFCE should connect more with other platforms/fora such as the UN processes to expand its visibility, identify organizations for partnerships, connect with technical entities with CCB knowledge and expertise and other global forums on cyber security.

Accelerating the adoption of Open Internet Standards

Speakers: **Olaf Kolkman** (GFCE Foundation Board/ISOC), **Maarten Botterman** (GNKS Consult)

The aim of this session was to share experiences from the adoption of the GFCE Internet Infrastructure Initiative which was established to raise awareness on open Internet standards with the aim of accelerating their adoption and implementation. This initiative is geared towards facilitating awareness raising and capacity building events in different regions in order to enhance justified trust in the use of Internet in those regions.

Olaf Kolkman opened the session and set the context for the presentation with statistics on deployment and implementation of standards and protocols aimed at increasing the security of the internet. These statistics highlight that deploying technologies is a voluntary measure as there are no mandated protocols in relation to internet. However, it is not visible for everyone that there is a positive benefit and deployment of standards is plagued by collective action problems. After this introduction, Maarten Botterman, facilitator of the Triple-I project 2018-2020 gave an overview of the GFCE Internet Infrastructure Initiative describing recent developments, including planned upcoming regional workshops and how the GFCE can best contribute to or facilitate ongoing efforts. GFCE Triple-I recognizes and is a response to the difficulties in acceleration adoption, deployment and implementation of internet security standards. It aims to take a regional and local approach to identifying solutions, helping participants to understand and identify which standards need to be deployed in their region and how stakeholders can be incentivized to act towards common goals. Whereas progress has been made since the start of the GFCE Triple-I initiative, it is clear that more work needs to be done to ensure the

best possible response by stakeholders in all regions to the current and upcoming challenges of teleworking. Lessons can be learned from global and regional practices, whereas keeping track of this and continuing to support global efforts fits very much within the scope of the GFCE. In the current iteration of Triple-I the Handbook on standards was updated and made available on the GFCE website alongside a playbook for building capacity building events and all reports from current and past events and workshops.

Working Together Towards a High-Level Cyber Capacity Building conference

Speakers: **Yurie Ito** (CyberGreen), **David van Duren** (GFCE Secretariat), **Sandra Sargent** (World Bank), **Chris Painter** (GFCE Foundation Board), **Tal Goodstein** (World Economic Forum), **Stéphane Duguin** (CyberPeace Institute).

With the launch of the GFCE during the Global Conference on Cyber Space (GCCS) in 2015, the importance of raising political high-level awareness of Cyber Capacity Building was underlined in the Hague Declaration. This is important to secure political recognition on cyber capacity building as: (i) a key enabler for digital development and (ii) a foundation for a prosperous digital ecosystem. The consultation session focused on raising awareness and support for such a conference and explored what the community would like to have included in the agenda of the high-level conference.

The panelists pointed out that the need of such a high-level conference can help improve the processes on cyber capacity building globally and will bring the CCB topic higher on the political agenda. Amongst the topics to be discussed in the conference, the panelists and participants mentioned the following: (i) national and regional coordination of CCB efforts, (ii) challenges in CCB, (iii) acknowledgement of CCB as equal to cyber security, (iv) redefine cyber policy development, (v) and how to secure CCB as a global issue. In order to raise awareness for organizing such a high level CCB conference it is important to create a strong coalition of global organizations, have concrete high-level deliverables, advocate the importance of CCB in the cyber space, engage high-level participation globally through a high-level committee. Furthermore, the importance of raising awareness on CCB being a critical issue on the development agenda of countries was stressed.