ANNUAL MEETING 2019

8 OCT > 10 OCT > ADDIS ABABA REPORT

GFCE
Global Forum on Cyber Expertise

Report on the GFCE Annual Meeting 2019 Addis Ababa

GFCE: Supporting Cyber Capacity Building for Growth

Everyone should be able to benefit from the potential that an open, free and secure internet has to offer. Under these conditions, cyberspace has thrived and continues to offer extraordinary opportunities for innovation, communication, sustainable development and economic growth. With the GFCE's unique structure as a bottom-up, neutral and apolitical forum, it provides an excellent opportunity for multi stakeholders to cooperate on cyber capacity building. The GFCE promotes cyber capacity building with a vision that the interests of security, economy and human rights go hand in hand.

The focus of the GFCE in 2019 is to further strengthen the structure for international cooperation on cyber capacity building. The GFCE can only be successful if the GFCE Members and Partners are involved and actively participate in steering the continuous development of the GFCE. The GFCE Annual Meeting 2019 in Addis Ababa was thus focused on working together with the GFCE community to bring the GFCE forward and to strengthen the global efforts of cyber capacity building.

The GFCE is honored that the African Union Commission hosted the GFCE Annual Meeting 2019 on October 8th-10th at the AUC premises in Addis Ababa, in parallel to the other international cyber-related events in the same week: the Commonwealth roundtable meeting, the public hearing of the Global Commission on the Stability of Cyberspace and the UNGGE regional consultations.

Table of Contents

Summary of the GFCE AM2019 outcomes

- **Delivering 11 Global workshops (organized by the Working Groups and the Advisory Board);**
- **Launch of Cybil, the renewed CCB knowledge portal (e.g. projects, tools, publications);**
- **Update on the GFCE Foundation and the GFCE Fund with the World Bank;**
- **Discussion on the GFCE developments and the way forward;**
- **New GFCE Advisory Board co-chair, Ms. Folake Olagunju Oyelola (ECOWAS);**
- **GFCE Women in Cyberspace Initiative;**
- **Organizations such as Chatham, UNODA and GCSC organizing their meetings on the sidelines of the GFCE Annual Meeting;**
- **Announcing the GFCE's 5th anniversary: meeting in The Hague in week of April 13th 2020**

DAY 0: WE SHARE

Tuesday 8 October 2019

The GFCE Working Groups and Task Forces demonstrated their added value through the workshops they have organized. These workshops are designed by and for the GFCE community, and provided the opportunity to share knowledge and expertise. All workshops had a focus on the African region and were open for all the participants of the Annual Meeting. Additionally, the GFCE organized a side-meeting on a West Africa coordination meeting and both a Sierra Leone and Senegal clearing house meeting.

Please find below a short recap of the workshops and side-meetings:

1.1 Cybercrime Law, Policy & Planning

Speakers: Mr. Zahid Jamil (WG C co-chair), Ms. Joyce Hakmeh (Chatham House/WG C co-chair), Mr. Matteo Lucchetti (Council of Europe), Mr. David Satola (World Bank Group), Mr. Moctar Yedaly (AUC), Ms. Allison Peters (Third Way).

Aim: To provide beneficiaries with useful insights and practical takeaways related to the need for having an anti-cybercrime strategy including important elements such as assessing the cybercrime landscape, long term Planning of acquiring capabilities to combat cybercrime, drafting Cybercrime Legislation, compliance with International Legal Frameworks and to create good Policies.

The workshop, moderated by Mr. Jamil, started with a presentation by the Council of Europe where Mr. Lucchetti elaborated on the GLACY+ project. This globally implemented program, funded by the EU, aims to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area. Key challenges according to CoE are Commitment of National authorities (on technical and political levels), Ownership (on both Cyber Security AND Cybercrime), Implementation (of Criminal Justice Capacity Building) and issues related to Fundamental rights and safeguards. Next speaker was Mr. Yedaly of the African Union Commission on the Malabo convention and the Digital Transformation Strategy (2020-2030) for Africa. The economic opportunities of ICT for Africa are tremendous and not to be missed, at the same Mr. Yedaly stressed that digital development does not go without cyber security and the capabilities to fight cybercrime. It is therefore an integral part of the DTS. Third speaker was the World Bank where Mr. Satola spoke on their international cooperation efforts with a broad range of stakeholders. A very practical tool on assessing the cybercrime landscape in one's country is freely available at www.combattingcybercrime.org. An updated version is expected in due time. Final speaker was Ms. Peters of Third Way, a Washington DC based think tank, and elaborating on a recently published study on effectiveness of Cybercrime Capacity Building. Findings and recommendations were shared and may serve as valuable input to the GFCE WG on Cybercrime.

1.2 Developing a national cyber security strategy

Speakers: Mr. Robin Bakke (Norway), Mr. Robert Collett (United Kingdom), Ms. Lea Kaspar (Global Partners Digital), Ms. Anat Lewin (World Bank), Mr. Kaleem Usmani (Mauritius), Mr. Kenneth Adu-Amanfoh (ACDRO).

Aim: The Strategy Workshop brought together experts with experience drafting national cyber strategies with those who are drafting strategies at the moment or considering doing so. The workshop contained four sections: starting the process; setting goals in the strategy; transitioning from planning to implementation; and how the GFCE can assist you.

Kenneth Adu-Amanfoh explained how Ghana started by gathering information and engaging with stakeholders. Robin Bakke and Lea Kaspar also emphasised the importance of stakeholder engagement: Norway wanted their strategy to be to "the most inclusive ever". Anat Lewin presented an overview of African national cyber strategies [slides available on Microsoft Teams] and gave her recommendations, including that there is a need for strategies to make better plans for monitoring and evaluation. Kaleem Usmani shared Mauritius' experience implementing their strategy, including the importance of identifying funding sources and Mauritius' commitment to international cooperation that will include a new regional centre of cyber excellence.

To conclude the workshop, the GFCE's task force for strategies and assessments explained how it can help you. The task force consists of GFCE community volunteers and is open to all GFCE members. It identifies good practice guides and tools that are shared through the Cybil Portal (**www.cybilportal.org**). It also connects those looking for assistance with members who can provide it, through a clearing house process. At the end of the workshop Robin Bakke said several international experts were available for one-to-one conversations about strategy drafting in the coffee breaks. Five African countries signed up to meet with them.

1.3 Internet of Things (IoT) Security

Lead: **Mr. John Hering (Microsoft), Mr. Solomon Kembo (ISOC), Mr. Dawit Bekele (ISOC), Mr. Mark van Staalduinen (TNO), Mr. Bill Newhouse (NIST).**

Aim: to show how governments can adopt IoT best practices.

The first introduction was done by Microsoft. Insight was given to the technology and lifecycle of IoT solution development to inform procurement and policy considerations. In particular risks of IoT, the different roles and responsibilities in securing an IoT device and regulatory trends and concerns were discussed. The importance of encouraging industrial competitiveness through IoT adoption and device certification were mentioned as examples. After that Solomon presented lessons learned from a project in Zimbabwe on developing an IoT controlled hydroponics system for urban farming. The project showed the successful use of IoT in controlling the environmebt (temperature, humidity, fish feeding, water level, etc.). Dawit presented the work of Internet Society in Canada and Senegal using a multi-stakeholder model to improve IoT policy and regulation. Their research showed that a majority of people are worried about lack of privacy and security in IoT. The importance to have a national framework on IoT was stressed. Mark van Staalduinen gave insight in the Global Good Practice Guide on IoT and the updated IoT Landscape Study. Both products are part of the cooperation between Singapore and The Netherlands on IoT and are available at the Cybil portal. The NIST's Cybersecurity for IoT Program was presented by Bill. Insight was given in the principles and the roadmap of the program. The importance of having trustworthy IoT devices by supporting manufacturers to identify and plan device cybersecurity and privacy features was stressed.

2.1 Cyber Incident Response

Speakers: **Dr. Sanjay Bahl (India) and Dr. Vilius Benetis (NRD Cyber Security)**

Aim: To lead to a deeper understanding of the challenges involved in an incident response scenario which is cross-sector and cross-border in nature. The aim of the incident exercise was to test both the incident management and policy decision-making skills.

The workshop started with an introduction on the Cyber Incident Response Lifecycle by NRD Cyber Security. This was followed by the interactive part of the workshop; a Scenario Based Interactive Exercise run by CERT-In and NRD Cyber Security. Participants were part of the National Crisis

Management Team of a hypothetical country, and each team had to formulate responses to several injects, divided over three different stages. In the third stage participants faced heightened threats, and had to respond and recover from Large Scale Incidents. With regard to enhancing *cross-sector* collaboration in countering these threats, key challenges such as awareness across sectors, political will, willingness to share information (e.g. the financial sector), ownership, trust and privacy, (external) media management, were highlighted. The exercise gave participants from countries which do not yet have a CSIRT an important understanding of the complexity of building out an incident response program. For participants from countries having a CSIRT, the workshop provided them with an insight of the gaps that may exist in their existing policy and / or engineering side as well as issues that may need to be addressed from a cross border perspective. During the next part in the session, CERT-In elaborated on applying a taxonomy for Cyber Security Exercises. The workshop succeeded by discussing the policy implications by NRD Cyber Security. During the workshop, all participants benefitted from learning about perspectives from both the policy and engineering side regarding cyber incident management.

2.2 Workforce development frameworks – The NICE Framework

Speakers: **Mr. Bill Newhouse (NIST), Mr. Owen Pierce (AustCyber) and Mr. Arkadiusz Kotowski (Palo Alto Networks)**

Aim: To provide beneficiaries with practical tools and guidelines on how to implement Workforce Development Frameworks in cybersecurity, with the NICE Framework as an example. The NICE Framework is a resource that categorizes and describes cybersecurity work.

The Workshop started with a presentation of the National Initiative for Cybersecurity Education (NICE) Framework, its components, and an introduction on how different audiences can reference it. AustCyber complemented with a presentation of the NICE Dashboard and Palo Alto showcased how the NICE framework was used to develop the Palo Alto Networks Cyber Security Academy Curriculum. The session concluded with a table top exercise whereas participants were asked to choose one NICE Framework Role and brainstorm on better use of wording to describe the role, whether there are gaps or non-relevance in the described knowledge skills and abilities and what is currently missing. Participants underlined the usefulness of the Framework and the adaptability to their organizational environments.

2.3 Open Internet Standards

Speakers: Mr. Arnold van Rhijn (The Netherlands), Mr. Alain Aina (WACREN), Mr. Michuki Mwangi (ISOC), Mr. Daniel Nanghaka (ILICIT Africa).

Aim: To raise awareness and share good practices on Open Internet Standards, such as HTTPS, DNSSEC and IPv6, on a regional and global level, specifically tailored to the African region.

In his introduction, workshop moderator Mr. van Rhijn gave an overview on what a model programme of a full-day expert meeting under the GFCE Internet Infrastructure Initiative (Triple I) does look like. Since 2018, these successful Triple I meetings are being organized in close collaboration with the local host and stakeholders in different regions of the world aiming to help build a robust, transparent and resilient internet infrastructure as well as to enhance justified trust in the internet by using the aforementioned standards. Panelist Mr. Aina then gave an introduction to the Open Internet Standards and local implementation of those standards. He was followed by Mr. Mwangi who shared the inspiration practice on Mutually Agreed Norms for Routing Security (MANRS). As last speaker, Mr. Nanghaka presented a Roadmap for Adoption of Modern Internet Standards in Africa. In particular, he showcased The-Internet.Africa, a platform which he is setting up to promote the adoption of the aforementioned standards in Africa following the example of Internet.nl, an online security testing tool initiated by the

Dutch Internet Standards Platform. Questions raised during the Workshop touched upon a.o. the use of modern internet standards by governments and securing financial support for the implementation process. Ultimately, the need to implement modern internet standards in a collaborative way was well-received.

3.1 Supply Chain Management in CIIP

Speakers: **Mr. Marc Henauer (Switzerland), Ms. Nynke Stegink (The Netherlands)**

Aim: The goal of this workshop was to create an understanding from both policy makers as industry representatives on how supply chain of critical information infrastructure can be managed best and which capacities are needed to do so.

The Workshop started with an instruction by Mr. Henauer and Ms. Stegink. This was followed by the interactive part of the workshop; a table top exercise on supply chain management in CIIP. During this table top exercise, the following three key questions were asked to the participants: 1. What are key supply chain cybersecurity challenges from a policy maker or industry perspective? 2. Which capacities are needed to identify and manage supply chains in regard to critical infrastructures? 3. What practices on supply chain cybersecurity can you share with the GFCE community? The session was concluded by a plenary part discussing the outcomes of the table top exercise. Participants learned more about the challenges and management of supply chain management in CIIP as valuable knowledge, best practices and experiences were shared among the participants.

3.2 Regional Cybersecurity Awareness campaigns

Speakers: **Mr. Miguel Canada (OAS) and Mr. John Hering (Microsoft)**

Aim: To provide beneficiaries with ideas, identify best practices, (existing) toolkits, and CCB initiatives regarding (regional) cybersecurity public awareness campaigns.

The workshop started with an informative session on how to make cyber awareness a priority. OAS presented the Cybersecurity Awareness Toolkit that displayed the main drivers: awareness process, campaign structure, -design and -implementation with a regional scope and countries support. Microsoft presented the Cybersecurity Tech Accord that highlights the importance of collaborating with private industry in developing and implementing awareness campaigns, which should strive to have the following characteristics: up-to-date, recursive, inclusive, culturally responsive, and multistakeholder. During the interactive session, participants reviewed and evaluated a case study of national cybersecurity awareness in the banking industry and identified next steps to develop a cybersecurity awareness initiative. The workshop succeeded in raising awareness among participants about the importance and impact of cyber awareness campaigns and provided a better understanding of the roles of different stakeholders in the development of these campaigns.

3.3 Shaping cyber policy through research and capacity building

Speakers: **Ms. Daniela Schnidrig (Global Partners Digital/GFCE Advisory Board), Ms. Grace Githaiga (Kenya ICT Network), Ms. Majama Koliwe (Association for Progressive Communications), Mr. Enrico Calandro (Research ICT Africa/GFCE Advisory Board), Mr. Muheeb Saeed (Media Foundation for West Africa); Ms. Lilian Nalwoga (Collaboration on International ICT Policy for East and Southern Africa)**

Aim: To discuss and explore how research and capacity building, conducted by civil society groups, can be leveraged in policymaking and used to influence and shape cyber policy outcomes at the national, regional and global levels.

The workshop, moderated by **Ms. Schnidrig,** was attended by a broad range of civil society groups as well as governments representatives from different African regions. There were lively discussions and several good examples were presented on how (local) research on the cyber landscape or specific cyber topics may contribute to government cyber security policy- and lawmaking. Through interactive discussions the exercise distilled a set of good practices (and challenges) that will be shared with the GFCE community.

4.1 Implementing Anti-Cybercrime Operations and Capabilities

Speakers: **Mr. Zahid Jamil (WG C co-chair), Ms. Nayelly Loya (UNODC), Ms. Lili Sun (INTERPOL), Mr. James Vigil (USA), Ms. Esther George (IAP), Mr. Tulumanywa Filbert Majigo (Tanzania), Mr. Terry Wilson (Global Cyber Alliance).**

Aim: To provide beneficiaries with practical examples by different stakeholders on implementing operational capabilities such as **Cybercrime Training**, **Legal Frameworks**, **Prevention tools** but also on the need for **International Coordination** of cybercrime capacity building. Practical takeaways were shared on best practices related to operational capabilities for combatting cybercrime.

The workshop, moderated by Mr. Jamil, started with a presentation by Mrs. Loya with an overview of UNODC's Global Programme on Cybercrime, which focusses on local and regional implementation. Ms. Sun elaborated on INTERPOL's Cybercrime Programme, which supports member countries to prevent and investigate cyberattacks. The Programme uses an Intelligence-led Operating Model consisting of 3 phases, Data Collation, Data Analyses (Cyber Activity Report), and Operation (Sharing, Support, Action, Training). Third speaker was Mr. Vigil on the US Transnational and High Tech Crime Global Law Enforcement Network (GLEN), which entails several programmes such as the International Computer Hacking and Intellectual Property advisors (ICHIP), the Global Cyber Forensics Advisors (GCFAs), and the Long Term Skills Mentoring by Investigator Trainers. All programmes aim to have a long-term commitment in several regions in order to have a sustainable impact. Ms. George explained the activities of IAP's GPEN (Global Prosecutors E-crime Network) such as webinars, and information letters to the community but focused in particular on the East Africa Regional Cybercrime Network (EARCN), a network of coordinators of 12 African states with shared objectives. Mr. Majigo shared his experience with EARCN and how it assists the Tanzania Prosecutor's Office. Finally, Mr. Wilson demonstrated the range of free available tools developed by the Global Cyber Alliance such as Quad9, DMARC, and Cybersecurity Toolkit for Small Business.

4.2 International Implications of Cybersecurity: Cyber Diplomacy, Norms, CBMs and CCB

Speakers: Ms. Kaja Ciglic (Microsoft) and Mr. Nikolas Ott (OSCE), Mr. Robert Collett (UK), Ms. Johanna Weaver (Australia)
Support: Ms. Elizabeth Vish (US), Mr. Chris Painter (WG A Chair), Ms. Carmen Gonsalves (the Netherlands)

Aim: To provide participants a greater understanding of international discussions on cybersecurity and the importance of these discussions for the national context. Participants were also able to reflect on their own involvement in national and regional cyber diplomacy efforts.

After a brief introduction on the dynamic cyber norms process, Mr. Ott and Ms. Ciglic highlighted the importance of regional efforts in supporting norms implementation and shared that the norms space is a thriving community where different stakeholders are engaged. To encourage further discussion, participants were split into six groups led by knowledgeable group leaders to discuss capacity building to implement a specific norm/CBM proposed by UN GGE 2015 (CIIP and CERTs), OSCE (CBMs on Information Sharing and Focal Points), and the Paris Call (Public Core of the Internet and Cyber Hygiene).

Stimulating discussions arose from these breakout groups and it was clear that a critical first step in grasping a norm/CBM is to define the scope. For example, looking at the UN GGE norm on CIIP, participants identified that challenges may stem from different definitions of critical infrastructures, different protection of one sector vs. another, absence of infrastructure framework, etc. To wrap up, Mr. Collett and Ms. Weaver shared their experiences in national capacity building for engagement in international cyberspace.

West Africa Coordination Meeting

On DAY 0, **seventeen funding and implementing organisations** held a West Africa coordination meeting. **ECOWAS assisted** with the preparation, but were unable to join. The organisations shared information on their activities with each West African country, and their regional projects. They focused on strategy/policy projects (Working Group A's theme), incident management and critical information infrastructure protection (WG B) and cybercrime (WG C), but noted projects in other areas too. The meeting **produced a table mapping all regional activities**, which will help with future coordination (please ask GFCE Secretariat if you would like a copy). The meeting discussed options for **a future Eastern Africa or Africa-wide coordination meeting**, including coming together in the margins of an event like Smart Africa or Africa IGF. The report of the meeting will be sent to ECOWAS to inform their regional coordination. Several attendees said that the meeting would help their programme planning and lead to further coordinating conversations among GFCE members.

Sierra Leone Clearing House Meeting

On DAY 0, **Sierra Leone's ICT Minister Swaray** met with the seventeen funders and implementers working in West Africa. He **presented Sierra Leone's clearing house priorities** for capacity building assistance: passing and implementing cybercrime legislation; public awareness campaigns; and establishing a national CSIRT. As a result of earlier clearing house discussions, the UK Home Office had already started providing support to a national cyber risk assessment (NCRA) to inform the national **strategy**. The Minister aimed to complete the strategy in January, with assistance from Global Partners Digital among others. Turning to **cybercrime**, the Council of Europe offered advice on the draft legislation, which the Minister would like to pass by the end of the year. The EU's OCWAR-C programme said they are working with ECOWAS to assist the region and stand ready to support Sierra Leone on cybercrime. Regarding **public awareness** campaigns, OCWAR-C's activity plan in Sierra Leone could include this. To respond to the request for **CSIRT assistance**, CTO and ITU said they had discussed how they would coordinate their support and agreed that the appropriate first step was a needs assessment and plan. PGI are co-delivering a national CSIRT training event in London on 9-11 December, to which Sierra Leonean officials will be invited. The World Bank are conducting a Digital Economy Assessment at the moment that will inform its future programming and can take account of the Minister's priorities. Minister Swaray thanked the group and stressed the importance of sustaining support into the implementation of the strategy.

Side-meeting Senegal Clearing House Request

The GFCE Secretariat has received a formal request from Senegal for GFCE assistance on two Working Group B related topics: 1. **A two-day workshop on a National CIIP Plan**; and 2. **The review of Senegal's 2016 CIRT Framework document**. The aim of this side-meeting was to continue the conversation, clarify and specify, and to identify possible next steps.

During this side-meeting, to which all Working Group B were invited, the status of Senegal's national (legislative) developments regarding the CIIP and CERT were discussed. Following this, both the CIIP and CERT requests for GFCE assistance were further clarified and specified. Next to this, past and ongoing CCB projects in Senegal related to CIIP and CERT, were discussed. By this, the side-meeting participants aimed to get further insight into identifying what could be done, what gaps remain and to identify next steps of the process.

Different suggestions were raised by the participants. An important outcome was that all participants emphasized the importance of including regional input regarding CERT/CIIP from African GFCE members when bringing in GFCE assistance. In addition, a representative from Senegal was invited to attend the Meridian Conference, held in Geneva from 14-17 October. Regarding action points, Senegal was asked to e.g. look into possible (legislative) challenges regarding the future establishment of a CERT, and share further details about the potential agenda of a two-day workshop on CIIP. The GFCE Secretariat will follow up and reach out to different GFCE members.

DAY 1: WE GROW

Wednesday 9 October 2019

Official opening

GFCE co-chair of the Netherlands, Ms. Carmen Gonsalves, Head of International Cyber Policies, Ministry of Foreign Affairs

Ms. Carmen Gonsalves opened the GFCE Annual Meeting 2019 in the Nelson Mandela Hall. She highlighted the importance of this year's Annual Meeting as it was the first time the GFCE met in Africa and to have representation from over 40 African countries. Additionally, she underlined that this is the first time that other organizations have chosen to hold meetings on the sidelines of the GFCE's Annual Meeting, such as the Global Commission on the Stability of Cyberspace, the UNGGE regional consultations and Chatham's roundtable session.

The title of this year's Annual Meeting is '**Supporting Cyber Capacity Building for Growth**'. It is important that everyone should be able to benefit from the potential that an open, free and secure internet has to offer in terms of innovation, communication, sustainable development and economic growth. As a unique structure, the GFCE as a bottom-up, neutral and apolitical forum, provides an excellent opportunity for multi stakeholders to cooperate on cyber capacity building. With a focus on cyber security, the GFCE promotes cyber capacity building with a vision that the interests for security, economy and human rights go hand in hand.

Ms. Gonsalves expressed that she looked forward to the remaining two days of the Annual Meeting and welcomed the new GFCE Members and Partners who have joined since last year's Annual Meeting in Singapore.

GFCE Advisory Board co-chairs, Mr. Patryk Pawlak, Brussels Executive Officer, EUISS – European Union Institute for Security Studies

Mr. Patryk Pawlak gave a short welcome on behalf of the GFCE Advisory Board to all the Annual Meeting participants. In his speech, he highlighted the importance of the GFCE's multi stakeholder approach and how the GFCE's Working Groups have an vital role in connecting the different stakeholders on various topics of interest. For the coming months, the GFCE Advisory Board will aim to further engage with the community and the Working Groups to help the GFCE grow.

Deputy Chairperson of the African Union Commission, H.E. Kwesi Quartey

H.E. Kwesi Quartey conveyed in his address the need for placing importance on Cyber Security, Online Privacy and Data Protection, Equity of Information, Confidence and Trust in the context of the African Union. He voiced that is a challenge to leapfrog digital development. The Deputy Chairperson emphasized the need of Cyber Security in Health, Agriculture, Education and handling of Cyber Crime and investigation. He underlined that development means that all African children are literate and numerate. The AUC's objective is to promote cybersecurity culture and to build trust and confidence in the use of cyber tools.

High level discussion panel on Cyber Capacity Building

- **Moderator: Head of Information Society Division /African Union Commission, Mr. Moctar Yedaly**
- **Officer-In-Charge of the Computer Emergency Response Team of Mauritius, Mr. Kaleem Usmani**

- **Head of Telecommunications at Economic Community of Central African States (ECCAS), Mr. Emmanuel Kamdem**
- **ICT Secretary in the Ministry of Information, Communications and Technology, Kenya, Dr. Katherine Getao**
- **Director of the African Regional Bureau of the Internet Society (ISOC), Dr. Dawit Bekele**

The aim of this high level discussion panel was to hear different stakeholders' perspectives on the current status of capacity building in Africa in the area of cybersecurity and cybercrime, and what the priorities are in this field for the different countries.

Mr. Emmanuel Kandem highlighted that he wants every country in Central Africa to have a national cyber security strategy and an implementation program. As a new member to the GFCE, ECCAS is looking to explore how the GFCE could assist with this ambition. Ms. Katherine Getao outlined her priorities in Kenya for cyber capacity building include CSIRT training and the importance of protecting critical networks. Ms. Getao also spoke about the need for regional discussions and cooperation, and reflected that more engagement is needed in cyber diplomacy. Mr. Kaleem Usmani reaffirmed Mauritius' commitment to promoting cybersecurity in the region. Mr. Dawit Bekele underscored that there needs to be more support for national cybersecurity efforts so that plans may come to fruition. Overall, everyone agreed that there is a real need to make cybersecurity more affordable, especially for developing countries.

In line with the AUC objectives as explained earlier by H.E. Kwesi Quartey, Mr. Moctar Yedaly shared that the AUC has decided to draft a digital transformation strategy for Africa, covering 2020 to 2030. The expectation is that this strategy will be adopted by the Head of State of the African Union in January 2020.

Announcements

Announcing the new GFCE Advisory Board co-chair

Both of the GFCE co-chairs, **Ms. Carmen Gonsalves (the Netherlands)** and **Mr. Ajay Sawhney (India)** were proud to announce that Ms. Folake Olagunju Oyelola, Program Officer Internet & Cybersecurity at the ECOWAS Commission, will become the new co-chair of the GFCE Advisory Board. The Advisory Board fulfills an important role within the GFCE as it represents civil society, academia and the tech community, and provides the GFCE with valuable and critical input.

Cybil – launch of the new CCB knowledge portal

The new CCB knowledge portal – Cybil – was officially launched by representatives from the Cybil Advisory Group: **Ms. Carolin Weisser-Harris (GCSCC), Mr. Ole Willers (NUPI), Mr. Gaus Rajnovic (FIRST) and Ms. Manon van Tienhoven (GFCE)**. The Cybil Portal is a one-stop knowledge hub that brings together resources and information on CCB from available open-sources and input from the GFCE community and broader knowledge partners. The Cybil Advisory Group presented the portal and discussed its vision and the future timeline. The portal is an extension of the GFCE's priorities: knowledge-sharing and coordination as it holds a wealth of information on projects, tools and publications. The portal is available on cybilportal.org.

Presentation of the 6th edition of the Global Cyber Expertise Magazine

Mr. Moctar Yedaly (AUC) presented on behalf of the Editorial Board (AUC, EU, OAS and GFCE), the sixth edition of the Global Cyber Expertise Magazine. The magazine features 10 articles that underscore practical CCB activities with a focus on international cooperation. This reflects an improvement in the coordination of CCB resources, knowledge-sharing and expertise around the world. The Global Cyber Expertise Magazine is available on the GFCE website.

Announcement from the United Kingdom

Mr. Alexander Evans **(UK)** announced that the United Kingdom is contracting £11m in new CCB services for international partnership projects: including with South Africa, Nigeria and Kenya. He also underlined the important role of the GFCE and that cooperation is key to improve global efforts on CCB.

Round-table work session 1: GFCE Progress

The first work session was held in a round-table format with a table leader at each of the 18 tables. After an introduction of the three topics through a short plenary pitch, each table used guiding questions to discuss two of the three identified topics. The following topics were introduced by these speakers: **CCB knowledge portal by Mr. Robert Newnham**, **CCB research agenda by Mr. Patryk Pawlak**, and **GFCE Working Groups by Mr. David van Duren**. The main outcomes of the session are mentioned below:

- **Cybil, the new CCB knowledge portal,** received great feedback. The overall opinion was that the new portal had a good foundation while there is certainly room for improvement. There are some important filters missing regarding the type of stakeholders (funder, beneficiary, implementer) as well as some important actors (civil society) and a clear mission statement. The groups provided new ideas to improve the taxonomy of the portal as well as its user interactivity (e.g. online discussion room or a chatbot function). The Cybil Advisory Group and the portal manager will work in the coming months to improve Cybil and to gather more content for the portal from the GFCE community.
- The idea for the GFCE to work on a **global CCB research agenda** was one of the outcomes of the GFCE Annual Meeting 2018 in Singapore. The input from the brainstorm session adds to the proposal that the GFCE Advisory Board has been working on. There are different ideas on how a GFCE research council can be formed, from a full time research manager in the Secretariat to having a role for the Working Group Chairs and/or GFCE co-chairs. Popular ideas for CCB research are metrics and a research project on how to improve CCB projects in the future (what works and what does not work in CCB).
- The GFCE Working Groups have been installed for almost 1,5 years. The community provided feedback on how the GFCE Secretariat could **improve both commitment as well as communication within the Working Groups**. Different ideas were presented: use Cybil as a tool for the Working Groups, more similar and formal processes for the Working Groups, and to give active Members and Partners more recognition for their work at a personal and organizational level. The GFCE Secretariat will work with the Working Group Chairs on ways to continue improving the Working Group process for 2020.

Round-table work session 2: GFCE Future Direction

The second round-table work session focused on the GFCE's Future Direction. During this interactive session, the GFCE community was given the opportunity to give feedback on the current plans and how they foresee the GFCE's next steps. Therefore, the aim of this session was to gather the opinions of participants in order to help the GFCE foundation board (in creation) and co-chairs in their overseeing roles. The session was introduced by **Mr. Christopher Painter**, who gave a short introduction on the two topics for discussion: **1) GFCE Scope of Content** and **2) GFCE Structure & Working Methods**. The main outcomes of the session are below:

- With the Delhi Communiqué in 2017, the GFCE created a common focus on the five CCB themes. The community provided feedback on whether there are **any topics missing in the GFCE scope of content** and that should be covered within the GFCE network. Almost each roundtable mentioned the importance of 'emerging technologies' (e.g. AI, blockchain, quantum computing, and 5G). This is something that is considered important enough to be covered by the GFCE in the near future. Additionally, other ideas came up, which will be shared with the Working Group chairs who will circulate it more broadly with their respective Working Group.

- The GFCE has three overarching objectives:
  1. *Improve efficiency and effectiveness: help share knowledge and expertise;*
  2. *Fill capacity gaps: help match requests from countries to offers of support (clearing house);*
  3. *Avoid duplication: help coordinate between projects.*

  The roundtable session focused on whether these objectives reflect the GFCE's current efforts and additionally, whether the community thinks that the GFCE fits in or should connect with other international or regional efforts (e.g. Paris Call or the IGF). The main feedback on the **GFCE's structure & working methods** was that the GFCE's efforts are reflected in our objectives but there is still room for improvement. There are certain CCB stakeholders not (properly) represented within the GFCE (e.g. private sector, cybercrime actors, regional organizations or civil society). Additionally, the GFCE should work on its branding and to clarify its strategic position compared to the other international efforts. This input, and the other insights collected by the Secretariat, will be used for the GFCE to work on its strategy for the coming year.

Breakout session on GFCE initiatives & CCB developments

1.1 Cybersecurity Capacity Building: A Cross-National Empirical Study

Speaker: **Prof William Dutton (University of Oxford)**

Professor William Dutton presented the outcomes of the Cross-National Empirical Study on Cyber Security Capacity Building. He demonstrated a summary of the findings related to the study's key research questions: 1. What is the status of national cybersecurity capacity building?; 2. What factors are shaping capacity building within nations?; and 3. What are the implications of capacity building for nations?. Important conclusions included the following: Cyber Security Capacity (CSC) shaped by the scale and centrality of the Internet along with the wealth and size of nations and their respective capacity for administrative changes. In addition, National choices on building CSC have implications for cybersecurity as well as the vitality of Internet use by individuals, business and government. This was followed by demonstrating the next steps in progressing the research. The participants were given in-depth insight into important aspects of cross-national Cyber Security Capacity Building, such as different stages of Cybersecurity Capacity Maturity, and the correlation coefficients for different categories, such as demographic, economic, infrastructure, and Political and Administrative System.

1.2 CSIRT Capacity Building

Speaker: **Mr. Koichiro Komiyama (JPCERT/CC Japan)**

Mr. Koichiro Komiyama presented on lessons learned from CSIRT Capacity building by looking at Japan's involvement in the establishment of PacCERT and AfricaCERT. PacCERT failed to survive due to the lack of finances to cover its operational costs and Mr. Komiyama identified the timeframe of 3 years that was allocated before handing over operational responsibility as being too short. AfricaCERT on the other hand is largely considered a success and it has been operational for 5 years with many stakeholders lending support. Mr. Komiyama reflected on his experiences and summarized that when establishing a CERT, three important factors you will need are focus, self-motivation, and endurance.

1.3 Stakeholder engagement in cybersecurity processes in Africa

Speakers: Ms. Lea Kaspar (Global Partners Digital), Mr. Adeboye Adegoke (Paradigm Initiative Nigeria), Ms. Grace Githaiga (Kenya ICT Action Network)

In this showcase GPD showcased the work they have done with civil society groups from the African region. There was an informal, dynamic conversation with participants from different organizations. GPD started with a presentation about GPD work which aims to facilitate effective participation of civil society in cyber policy debates at the national, regional and global levels, and to make cyber policy development processes more open, inclusive and transparent. This was followed by a presentation of Mr. Adegoke on his Paradigm Initiative's Digital Rights program in Anglophone West Africa, where he focuses on research and strategic advocacy implementation. His work focus is advocacy for equity and human rights online. After that Ms. Githaiga made a short presentation on the Kenya ICT Action Network (KICTANet), a multi-stakeholder platform for people and institutions interested and involved in ICT policy and regulation. Finally an overview was given on the ongoing initiative to develop a publication which highlights good practices in stakeholder engagement in Africa.

2.1 Senegal Cybersecurity developments

Speaker: **Ms. Racky Seye (Senegal)**

Ms. Seye demonstrated the Senegal Cyber Security Strategy, "SNC2022". First, the cybersecurity landscape was presented, including information on the (national) legal and regulatory framework, instructions and circulars, and conventions. An interesting highlight is the fact that Senegal ratified both ratify the African Union Convention on Cyber Security and Protection of Personal Data, and the Budapest Convention on Cybercrime. Following this, Ms. Seye elaborated on Statistics, the National Cybersecurity Strategy drafting process and the achievements and challenges of Senegal regarding cybersecurity. The break out session was concluded by Mr. Koyabe (CTO), who elaborated on CTO's experiences with developing Senegal's National Cyber Strategy as implementing partner, funded by the Netherlands. Participants were enlightened on the achievements and challenges with regard to the cybersecurity developments in Senegal.

2.2 Capacity Building Efforts of France in Africa: a School of Cybersecurity in Senegal

Speaker: **Mr. Stephane Le Brech (France)**

Mr. Stephane Le Brech presented France's active involvement in building cyber capacity in Africa. In 2017, France announced the creation of a school of cybersecurity in Africa to fight cybercrime and assist with cyber strategies. Working closely in partnership with Senegal, the National School of Cybersecurity with a regional orientation was installed in Dakar in 2018. The school is planning to start regional training sessions by the end of 2019 and provide a full training program in 2020 with subjects such as governance of cybersecurity, security of information systems, fight against cybercrime and digital intelligence. Mr. Le Brech also discussed the partnerships that were formed to make this school possible (both national and international), highlighting the need for collaboration in implementing concrete cyber capacity building initiatives.

2.3 Development of National Level Cyber Health Annual Check-up Analysis

Speakers: **Ms. Yurie Ito (CyberGreen)**

In this showcase Ms. Yurie Ito presented program development of her organization CyberGreen. Over time, the medical community has identified things worth measuring for preventative measures. Similar to human health, CyberGreen is developing the metrics framework to measure Cyber ecosystem healthiness. CyberGreen develops robust metrics to measure Cyber Health and Hygiene in a nation. It collects and analyzes data for five open recursive protocols (NTP, DNS, SSDP, SNMP, CHARGEN) commonly used to execute DDoS reflection attacks. These open servers have the potential to be used as infrastructure to launch DDoS attacks within a country's borders and abroad. In addition CyberGreen conducts a Cyber Health check-up and analyzes policy and mitigation needs for improvement. Finally network operators, policymakers and other stakeholders are informed on the risks associated with hosting open servers. The metrics framework will be further developed and extended soon by adding new Health Risk Indicators and Security Performance Indicators. CyberGreen will soon perform Cyber Health analysis for 10 ASEAN countries and kindly invites the GFCE community for further cooperation.

3.1 Improving cyber security through Table-Top Exercises: Czech view on how to design TTXs

Speaker: **Mr. Jakub Otčenášek (Czech Republic)**

Based on the experiences of the Czech Republic, Mr. Otčenášek elaborated on the conduction of cyber security exercises as important learning tool for many institutions and business. The geographical aspects and types of cybersecurity exercises were discussed and demonstrated a video on NÚKIB's cybersecurity exercises. Finally, the advantages of conducting cybersecurity exercises were highlighted. They can help to raise awareness, test procedures and build competence and relationships. At the end of the workshop, Mr. Otčenášek handed out NÚKIB's Handbook "How to Develop a Cyber Security Table-Top Exercise" to all participants. This handbook is a deliverable of the GFCE Working Group B and provides context and guidance for planning, developing, organizing and improving cyber security table-top exercises. Participants learned how government and other entities involved in enhancing cybersecurity can stay ahead of evolving threats by cybercriminals and hackers, by learning more about the experiences and expertise of NÚKIB regarding cybersecurity exercises.

3.2 International Cyber Discussions: understanding the GGEs and OEWG

Speakers: **Ms. Kerstin Vignard and Ms. Camino Kavanagh (UNIDIR)**

During this session led by UNIDIR's Ms. Kerstin Vignard and Dr. Camino Kavanagh, the audience learnt about the history of intergovernmental cyber discussion in the UN and were given the opportunity to ask questions related to the GGE and OEWG. Ms. Vignard presented a brief history of the GGE and OEWG including the structure of the groups, their different modes of operation, the outcomes of previous GGEs and recent developments. While a consensus report was not produced after the fifth GGE session in 2017, Ms. Vignard highlighted that this does not signal failure because progress was made in identifying CBMs and other capacity building efforts. CBMs are especially important as launch pads that facilitate and strengthen dialogue on norms. Inclusivity of non-governmental actors in the international norms process and the mechanism for which such stakeholders be involved was also discussed. Additionally, the role of UN GGE regional consultations was emphasized as an inclusive process aiming to engage and spread awareness in the region – the group conducted their African regional consultation on Friday, 11 October.

3.3 Implementing Cyber Strategy: Tips for Organizing at the National Level

Speakers: **Ms. Johanna Vazzana (MITRE Corporation)**

In this showcase Ms. Johanna Vazzana presented lessons learned and suggestions for how governments and national stakeholders can organize around strategic goals to help ensure successful strategy implementation program. The most important aspect of having a National Cyber Strategy is its determined and successful implementation. Publishing a strategy does not end, but rather starts the real work, and a successful national cyber strategy requires a continuously on-going process of assessment, development, and implementation. Two topics were discussed: effective cyber governance structures and the establishment of a national cyber coordinator role.

4.1 Kenya Cyber Capacity Building developments

Speaker: **Dr. Katherine Getao (Kenya)**

Dr. Getao elaborated on the topic of cyber capacity building in Kenya, for which she discussed different areas of success: technical cybersecurity expertise, the education sector, the public sector and the private sector. Regarding technical cybersecurity expertise, there was elaborated on 61 universities offering cybersecurity programs at the graduate level. For the education sector, Dr. Getao discussed the challenges and opportunities regarding cybersecurity education for primary and secondary schools. In addition, ways of cooperation and improvement of that cooperation with the private sector was discussed. Next to the learning part for participants on Kenya's cyber security landscape, the break out session had an interactive character. As Dr. Getao encouraged participants to share their inputs, an important outcome of the break out session were the valuable discussions and exchanges of knowledge and experiences among the participating countries and institutions.

4.2 Bringing stakeholders together: the GFCE Triple-I experience

Speakers: **Mr. Maarten Botterman (ICANN)**

How to progress a more robust Internet in the region by awareness raising, inspiration and collaboration? Organize a GFCE Triple-I workshop! In this showcase Mr. Botterman presented the overall experience and results of the GFCE Triple-I project elaborating on the success formula behind the GFCE Triple-I capacity building workshop, and how this has worked out in practice during the 6 workshops that have taken place around the world, so far. The aim of this initiative is to help build a robust, transparent and resilient internet infrastructure. Following the experience in the Netherlands in testing and monitoring compliance with international internet standards, this Initiative seeks to broaden this know-how. Key elements include building on state-of-the-art Open Internet Standards and good practices in improving the reliability of the Internet.

4.3 ASEAN-Singapore Cybersecurity Centre of Excellence

Speaker: **Mr. Sithuraj Ponraj (Singapore)**

Mr. Sithuraj Ponraj from the Cyber Security Agency of Singapore presented the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), launched one week prior during Singapore's fourth International Cyber Week. The ASCCE is an extension of Singapore's 2016 ASEAN Cyber Capacity Programme (ACCP) with the aim to build the region's collective capabilities in cyber policy, strategy development and technical/operational areas (e.g. CERTs and incident response). Recognizing that hit and run capacity building programs are not favorable as there is no charted progress, the ASCCE's training program will be delivered holistically consisting of 50% policy and 50% technical areas with a "3M" approach: multi-stakeholder, multi-disciplinary and modular. Mr. Ponraj drew attention to a fourth "M": metrics, and shared that the development of a framework to assess the effectiveness of such training programs is necessary and currently in the works. The session gave insight on the regional developments and collaborative efforts in cyber capacity building amongst the ASEAN countries.

Closing remarks

GFCE co-chair of India, Mr. Ajay Sawhney, Secretary, Ministry of Electronics and Information Technology

In his closing remarks, Mr. Secretary reflected on a successful GFCE Annual Meeting. He underlined that the GFCE Annual Meetings are unique in its nature. Besides the different opportunities to refresh relations and to discuss the problems of mutual interest, it encourages the sharing of relevant experiences and to find ways to cooperate to help each other. Mr. Secretary hopes that these meetings will continue to highlight additional avenues for cooperation within the GFCE community and propose beneficial, cutting-edge resolutions which can positively impact cyberspace.

GFCE Working Group and Task Force meetings

The focus of Day 2 of the Annual Meeting was WE IMPLEMENT. The day was dedicated to the GFCE Working Groups and Task Forces meetings to discuss the direction of the WGs and supporting the practical implementation of CCB
The GFCE Working Groups and Task Forces had side-meetings throughout DAY 2. Full reports of these meetings are available on GFCE Microsoft Teams. Please find below a short overview of the accomplishments of the Working Groups and their deliverables for 2020.

	Accomplishments 2019	**Proposed deliverables 2020**
WG A – Cyber Security Policy & Strategy	- WG A is the only working group that has received formal requests of support through the clearing house mechanism. Progress has already been made in assisting Sierra Leone (national CS strategy) and Tunisia (national CS assessment), and the Gambia has just submitted their formal request. - After listening to the needs of the WG, two Task Forces (Strategies & Assessments; CBMs, Norms implementation & Cyber diplomacy) were established to give the needed focus and guidance to these two important areas.	- The TF on CBMs/norms would like to explore how it can be of added-value to international processes on cyber norms and the norms discussion - A catalog of offers for support has been drafted by the TF on Strategies. The WG will refine this and create a catalog for the TF on CBMs/norms as well. - As the two task forces have only recently been established, the WG will work on creating synergy and harmony between them.
WG B – Cyber Incident Management & Critical Information Protection	- Regarding Coordination, both Task Forces would like to continue its work to identify useful publications, resources, tools and CCB projects to be put on the Cybil – CCB knowledge portal. - Both Task Forces organized successful workshops on Cyber Incident Response and on Supply Chain Management in CIIP. Additionally, both Task Forces published a framework: Global CSIRT Maturity Framework and a CIIP Framework. - Senegal is the first clearing house request of the Working Group, the request has been specified and follow-up will be given in the coming months.	- Application of WG B products and (proposed) New Work Areas, both working in small projects teams. The plan is to set up smaller project teams within each Task Force, focused on the application of WG B products and/or develop proposals for newly proposed topics. For CIIP, proposed topics include. : Deepening on the CIIP Framework: supply chain/ stakeholder management; Practical application & testing of Framework and guides; Deepening into smart security (Cities/ Airports/ Harbours); and Criticality of data. For CIM, proposed topics are. : Developing a new national CERT (Day 0 CERT) as an extension of the maturity framework work, CERT Hierarchy Mapping, fostering stronger national CERT to organizational CERT relationships, Integrating 'Protecting SMEs' & 'IoT' work being done at APCERT, Next Generation CERT competencies, NCSC 1-pager. - Intensify mapping: WG B encourageS each country / participant will write a 2-pager on where they are on CIM and CIIP. - Populate the Cyber Capacity Building (CCB) Portal – Cybil - Streamline and establish the WG B clearing house process

		- Coherent sharing between the Working Groups e.g. Supply Chain IoT; possible implementation of Work Group A outputs like Strategy; and Emerging Technology (e.g. AI and IoT), in cooperation with WG E.
WG C – Cybercrime	- Creating an informal network of key organizations working on cybercrime capacity building projects around the world which has been facilitating the exploration of synergies between these organizations as well as cooperation opportunities. - Supporting the World Bank and the Korean Supreme Prosecutor's office in launching a regional cybercrime hub for Asia-Pacific. A memorandum of understanding between the Prosecutor's office, the WB and the GFCE will be signed in November of 2019.	- Developing clear mechanisms for each of the Working Group functions (coordination, knowledge sharing, clearing house and research agenda) with a clear timeline and process for how partners and members can input into the Group's work and receive the necessary support when needed. - Working on an engagement plan for the WG participants to ensure their proactive participation in shaping the strategic direction of the WG. The plan will be tailored to reflect the needs of the different sub-groups which include governments, donors, implementers and others. - Enhancing the coordination with the other GFCE working groups on a systematic basis in order to deconflict when necessary and share lessons learned and best practices.
WG D – Cyber Security Culture & Skills	- Both Task Force of WG D have organized successful workshops on workforce development and on awareness campaigns. - The WG has received multiple expressions of interest, mostly from non-GFCE Members, it is key that countries become a member of the GFCE before they can enter the clearing house request. In turn, the WG aims to further establish its clearing house process and efforts. - The WG has done an extensive mapping exercise already which served as input for two White Papers.	- WG D will continue its mapping exercise to adhere to the GFCE's mandate to share best practices and to avoid duplication of efforts. - There are two ideas to develop standard support packages in WG D, one is on workforce development and the NICE framework could be an example for this. The other idea is on Awareness campaigns combining the OAS awareness campaign toolkit with other campaigns and lessons learned. - A first idea for the CCB research agenda is about that in current awareness campaigns important sectors are missing, e.g. the public health sector.
WG E – Cyber Security Standards	- For the Annual Meeting 2019 two workshops were developed / organized: a workshop on IoT & a workshop on Open Internet Standards. - The Working Group did a mapping exercise on IoT knowledge products, relevant IoT frameworks and relevant IoT organizations / implementers. - A grosslist of 50 IoT resources were selected; - About 20 products are selected for the CCB portal. - A Global Good Practice Guide with several good practices, that can be put to use by officials that aim to enhance IoT security, was developed.	- The Working Group will act as a clearing house for useful products / tools /projects for the Cybil Portal on the topics of IOT/Internet standards. Knowledge will be collected from the Working Group and other sources like the IGF best practice forum. - IoT Highlights/Events Calendar. For Working Group Members a IoT highlights/events calendar will be developed in order to stay in the loop on relevant IoT highlights and/or events. - An overview will be given, outlining the needs and interests of involved stakeholders in the Working Group. A pilot for the clearinghouse (support a need) will be conducted. - Based on the Triple I meetings a standard package will be developed with knowledge, tools (internet.nl) and lessons learned on internet standards. - Two pilot case studies will be executed as a way to share best practices for actors in need for assistance in the same case setting.