Report on the GFCE Annual Meeting 2018 Singapore

From Awareness to Implementation of Cyber Capacity Building

The Global Forum on Cyber Expertise (GFCE) was launched in 2015, during which time it was anticipated that the GFCE would develop into a global, informal and coordinating platform for Cyber Capacity Building. Nowadays the GFCE functions as an ecosystem that enables efficient international cooperation in building cyber capacities. The role of the GFCE as global implementing platform for CCB (a clearinghouse for knowledge, expertise and funding) will become increasingly important. During the Global Conference on CyberSpace 2017, the endorsement of the Delhi Communiqué on the GFCE Global Agenda for Cyber Capacity Building was the starting point of the CCB implementation process.

The GFCE Annual Meeting 2018 has focused on the positioning of the GFCE as the facilitating and coordinating platform on the knowledge and expertise sharing for the implementation of cyber capacity building.

The GFCE is honored that Singapore hosted the GFCE Annual Meeting 2018 on September 18th-20th at the Marina Bay Sands Expo and Convention Centre in parallel to the 3rd edition of the Singapore International Cyber Week.

DAY 0 - Tuesday 18 September 2018

Following the Grand Opening of the 3rd Singapore International Cyber Week on Tuesday September 18th, the GFCE organized its Day 0 of the GFCE Annual Meeting in the afternoon at the Marina Bay Sands Expo and Convention Centre.

This day included several parallel meetings and served as an introduction to the Annual Meeting. These were **GFCE Working Group meetings** on the different cyber capacity building themes identified in the Delhi Communiqué: *Cyber Security Policy & Strategy; Cyber Incident Management & Critical Information Protection; Cybercrime; Cyber Security Culture & Skills; and Cyber Security Standards*.

Additionally in collaboration with Singapore and the Netherlands, the **International Internet of Things (IoT) Roundtable session** was organized in the afternoon for the second year in a row.

The GFCE Secretariat, in collaboration with the World Bank, also organized the **Africa Regional Meeting**. This closed session succeeded the first GFCE - World Bank Africa regional meeting held in Uganda, back in June 2018. The aim of the Africa Regional Meetings is to bring together different GFCE stakeholders who are active in cyber capacity building (CCB) in Africa. Several experts introduced topics with a focus on Cyber Security Strategy, CERTs and Cybercrime legislation. This was followed by a discussion on a mapping exercise, which aims to assess needs and to direct the discussion towards assistance from the GFCE community.

DAY 1 - Wednesday 19 September 2018

Opening GFCE Annual Meeting 2018: *"From Awareness to Implementation"*

Welcome by the GFCE co-chairs

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

Mr. Secretary opened the GFCE Annual Meeting. He elaborated that, since 2015, the GFCE has provided a valuable space to ensure that all nations can embrace an ever-expanding cyberspace. Mr. Secretary underlined that India sees cyberspace, "as an ecosystem that emerging digital nations can leverage to transform the lives of people through good governance. People are encouraged to embrace the Internet through a trusted ecosystem". This is why a platform as the GFCE is important, since the GFCE creates an ecosystem that enables efficient international cooperation in building cyber capacities.

He continued that in 2018, the GFCE Secretariat has identified three key priorities, which are crucial for the further development of the GFCE:

1. Development of GFCE Working Groups along the lines of the five prioritized themes of the Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building;
2. Establishment and development of a Global CCB Knowledge Partner Network, which is essential for the contribution of the practical knowledge and implementation expertise to the GFCE network;
3. Further internationalization of the GFCE and the Secretariat.

Mr. Secretary was pleased to inform the audience that these key priorities returned on the agenda during this GFCE Annual meeting.

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

Subsequently GFCE co-chair of the Netherlands, Ms. Carmen Gonsalves, looked forward on the two-day agenda of the Annual Meeting and welcomed the new GFCE Members, Partners and initiatives, who joined since last year's Annual Meeting. Kindly find an overview below:

New GFCE members:

- From the African region, we welcome: Mauritius, Ivory Coast, Nigeria and Gambia.
- From the European region, we welcome: Austria and the Czech Republic.
- From the Asian region, we welcome: the Philippines and Thailand
- From the Central and South American region, we welcome: Guatemala and Dominica
- Lastly, we welcome FS-ISAC.

New GFCE partners:

- The Center for Cyber Security and International Relations Studies (CCSIRS)
- Global Partners Digital
- Potomac Institute for Policy Studies
- EastWest Institute
- IPANDETEC
- NUPI
- ECTEG
- ASPI
- Cybersecurity & Cybercrime Advisors Network

New GFCE initiatives;

- No More Ransom
- Promoting the implementation of tools & frameworks to enhance cyber stability between States
- e-Government and Cybersecurity in Latin America and the Caribbean
- CyberSouth Project
- IoT Security initiative
- Cyber Surakshit Bharat initiative

Keynote Singapore

- **Mr. Teo Chin Hock, Deputy Chief Executive (Development), Cyber Security Agency Singapore**

The opening session of the GFCE Annual Meeting was concluded with a key note, from the host of the GFCE Annual Meeting 2018. The year 2017 saw an increasing interconnectivity, with the ubiquity of Internet-of-Things (IoT) and other Smart technologies. This is a rising trend, which holds tremendous potential for economic progress and the rise of living standards across the globe. At the same time these technologies call for being supported by strong cybersecurity measures, especially so in the case of supranational Critical Information Infrastructures where the effects of a successful cyber-attack or cybercrime actions can have far-reaching and disproportionate knock-on effects on other countries around the region and the globe.

However, cyber capabilities differ from country to country – and develop at vastly different rates. Singapore stresses the importance of cyber capacity building across a broad range of areas. This should be achieved in a coordinated manner that seeks to complement existing global and regional initiatives to avoid duplication of efforts.

In addition, it is also important for Singapore to cooperate as an international community on cyber capacity building. In this regard, it is clear that the GFCE has an important role as a global platform to exchange best practices and expertise on cyber capacity building.

Panel discussion: Future of global CCB cooperation

- **Moderator: Ms. Alison August Treppel, Executive Secretary Inter-American Committee against Terrorism (CICTE), Organization of American States (OAS) (OAS)**
- **Mr. Robert Strayer, Dep. Assistant Secretary for Cyber and International Communications and Information Policy, Bureau of Economic and Business Affairs, US Department of State;**
- **Ms. Folake Olagunju Oyelola, Program Officer Internet and Cybersecurity, ECOWAS;**
- **Ms. Angela McKay, Senior Director of Cybersecurity Policy and Strategy in the Global Security Strategy and Diplomacy team, Microsoft;**
- **Mr. Tobias Feakin, Ambassador for Cyber Affairs, Australia**

The aim of the opening panel discussion was to reflect from different stakeholders' perspectives on the significance of global cooperation on cyber capacity building and on how this cooperation can be improved in the (near) future.

Ms. Folake Olagunju Oyelola underlined that there a few who decide all in cyber capacity building. It was advised to take a step back in order to contextualize the local/regional environment. Important step to make is to change the modus operandi, cyber security academic programs and awareness campaigns can be helpful in achieving this. The panelists reflected that it is essential that the funding and implementing stakeholders need to understand the region's specific requirements to customize the cyber capacity programs.

The representative from Microsoft, Ms. Angela McKay, highlighted that the donor commitment does not necessarily match the needs of recipients. Therefore, Ms. McKay called for a more coordinated approach to cyber capacity building with a balanced perspective,and stressed theimportanceof public-private-partnerships.

The overall message was that there is a need for more coordination in the field of cyber capacity building and that a truly multistakeholder approach is key to achieve this. The GFCE is an important vehicle in connecting different stakeholders to facilitate further cooperation in the field of cyber capacity building. A possible future mechanism for the GFCE is to develop a feedback mechanism to continuously improve and adapt future cyber capacity building programs.

Presentation of the GFCE Advisory Board 2018-2020

- **GFCE Advisory Board co-chairs, Ms. Rooba Y. Moorghen, Permanent Secretary, Ministry of Technology, Communication and Innovation in Mauritius and Mr. Patryk Pawlak, Brussels Executive Officer, EUISS – European Union Institute for Security Studies**

As per June 1st 2018, the new GFCE Advisory Board was officially installed. The AB co-chairs, Mr. Patryk Pawlak, Brussels Executive Officer, EUISS as well as Ms. Rooba Y. Moorghen, Permanent Secretary, Ministry of Technology, Communication and Innovation in Mauritius, introduced the GFCE Advisory Board and it's plans for the coming year, to the GFCE Community.

Mr. Pawlak stressed that after a period of expansion and deepening it is time to deliver results and demonstrate added value of cyber capacity building through the GFCE. The Delhi Communiqué and the establishment of the Working Groups provide one of the frameworks for doing so. The AB intends to become a marketplace of ideas for the GFCE community and a one-stop-shop for strengthening engagement between GFCE Members and other stakeholders. This might result from time to time in speaking the inconvenient truth about the state of the GFCE community.

Consequently, the AB intends to become more active in three areas:

- **Proactive engagement with the GFCE community** with a unique voice based on the inputs from a broader community e.g. through the participation in the WG's and views on new membership proposals and initiatives under the GFCE umbrella.
- **Engagement with stakeholders** by defining its modalities for outreach and engagement with various communities and regions whereby individual members assume a more active role within their communities.
- **Strategic communication** by developing a strategy for communicating its work and ensuring that the AB's voice is heard.

Finally, Ms. Moorghen added several concrete actions by the AB for the near future, such as:

- Concrete recommendations to the WG's;
- Efforts to expand the membership of nations from underrepresented regions;
- Create synergies and multiply impact of the ongoing GFCE initiatives;
- Identify ways for improving cooperation with the private sector and civil society and;
- Support and integrate into our work the experience and expertise already available in various regional expert hubs as capacity building multipliers.

For an overview of the individual GFCE Advisory Board members, please visit the GFCE website.

Roundtable discussions 1: GFCE Working Groups

The GFCE encourages interaction between the different stakeholders and therefore similar to last year, on both Day 1 and Day 2, roundtable discussions were taking place. On Day 1, the roundtable discussion focused on the progress and ambitions of the GFCE Working Groups. The aim of the session was to involve non-Working Group participants in the processes of different Working Groups and to define some key take-aways from the GFCE community. A different Working Group was discussed per table in each round. Either a Working Group chair or a representative led the discussion at each table.

The roundtable session resulted in new ideas and comments on the progress of the respective Working Groups, which the Working Group chairs will take into consideration in the coming weeks. The roundtable discussion brought several insights that are applicable to all the Working Groups. Kindly find a short overview below:

- **More harmonization** between the five Working Groups. This can be realized through different channels:
    - A 'harmonized agenda' for the Working Groups with similar building blocks;
    - Involvement of the Advisory Board members to share knowledge and feedback cross-cutting through the Working Groups;
    - A quarterly Working Group Chairs call / meeting;
    - Online workspace, e.g. Microsoft Teams.
- **More transparency** between the Working Groups, e.g. sharing of the process as well as the outcomes with the GFCE community.
- **More awareness** of the Working Groups outside the GFCE community and more outreach:
    - Missing stakeholders: recipient countries, private sector, and academia.

GFCE initiatives and showcases

During each GFCE Annual Meeting, both GFCE as well as non-GFCE members and partners have the opportunity to showcase their initiatives / work related to global cyber capacity building.

Location:	***Angsana 3D***	***Angsana 3E***	***Begonia Junior 3010A/B***
14.30 – 14.55	***IoT Security initiative*** Singapore & Netherlands	***National Cyber Security Guide*** CTO, ITU, Microsoft, World Bank, GCSCC, Deloitte	***Recommendations on practical futures for cyber confidence building in the ASEAN region*** ASPI
15.00 – 15.25	***CSIRT Maturity / CIIP*** Spain, Switzerland, Norway, Netherlands	***World Bank's Digital Development Partnership (DDP)*** World Bank	***Charter of Trust*** Siemens
15.30 – 15.55	***INTERPOL's Cyberspace and New Technologies Lab*** INTERPOL	***The Cyber Surakshit Bharat Program*** India	***Cisco Networking Academy*** Cisco Systems

International IoT security initiative: Global approach towards the adoption of IoT security policies and solutions

- **Mr. Lim Soon Chia, Director Technology, Cyber Security Agency of Singapore**
- **Mr. Geert Moelker, Manager Telecom Markets Directorate, Netherlands Ministry of Economic Affairs**

IoT devices are increasingly introduced on the market without a basic security level and this could lead to exposed vulnerabilities during their unknown lifespan. With the rapid proliferation of IoT where physical objects are becoming smart and connected, threats are also no longer geographically bound, and are becoming more sinister with widespread repercussions for governments, businesses and everyday users. Therefore, it is pertinent to create an ecosystem that is secure from design to disposal; a challenge that requires a global approach. The objective of the initiative is to provide Public and Private a level of understanding and guidance in order to accomplish a more secure IoT environment by creating successful policies, good practices and practical solutions to solve the cross-domain and cross-functional challenges of IoT security. Three main topics are identified to realize these objectives*:* IoT Evaluation and Certification Regime(s), Trusted Supply Chain and Trusted Identity.

Interested GFCE members and partners may contact the GFCE Secretariat.

National Cyber Security Guide

- **Ms. Kaja Ciglic, Director, Government Cybersecurity Policy and Strategy, Microsoft**
- **Ms. Sadie Creese, Founding Director of the GCSCC, Oxford**
- **Mr. Marco Obiso, Head ICT Applications and Cybersecurity Division at ITU**
- **Mr. Andrea Rigoni, Partner in Deloitte Risk Advisory**
- **Mr. David Satola, Lead Counsel, Technology and Innovation at World Bank**
- **Ms. Sandra Sargent, Senior Operations Officer, Digital Development, World Bank**

This multi-stakeholder initiative presented its Guide to developing a National Cybersecurity Strategy. The document offers a unique resource, a framework agreed on by organizations with demonstrated and diverse experience in the topic and builds on their prior work in this area.

Purpose is to guide national leaders and policy-makers in the development of a National Cybersecurity Strategy. The guide focuses on protecting civilian aspects of cyberspace. It does not cover aspects related to developing offensive and defensive capabilities. It does provide indications on “what” should be included in a National Cybersecurity Strategy, as well as on “how” to build, implement and review it. Key elements in the guide are the lifecycle of an NCS, a set of overarching principles and an outline of NCS Good Practices divided into several focus areas. The NCS guide is **available online**.

Recommendations on practical futures for cyber confidence building in the ASEAN region

- **Mr. Bart Hogeveen, Head of Cyber Capacity Building**

In this session, the Australian Strategic Policy Institute (ASPI) presented the "Sydney Recommendation on Practical Futures for Cyber Confidence Building in the ASEAN region". The recommendations are the outcome of a series of consultations between the region's Track 2 institutions and a public round table meeting in Sydney in March 2018, as part of ASEAN-Australia Week. The document provides a set of practical steps that stakeholders in the ASEAN region can take with the aim of reducing and eliminating causes of mistrust, fear, misunderstanding, and miscalculation that may stem from the use of ICTs. The document is **available online**.

CSIRT Maturity / CIIP

- **Ms. Petra Timmers, Coordinating Policy Officer International Cyber Policies, Netherlands Ministry of Foreign Affairs**

CSIRT Maturity Framework Initiative

This GFCE Initiative will make available to the worldwide community of national/CIIP CSIRTs a framework that they can use to increase their CSIRT maturity in a structured and step-wise approach. This framework will be based on the SIM3 maturity model and the ENISA step-wise approach that was built on top of SIM3. This model and approach are firmly planted in the daily reality of national teams all over the world. It has proven to be highly successful in Europe, Japan and is currently gaining in popularity. The idea is not to prescribe one way of assessing and improving maturity, but rather to endorse this framework as good practice and make it readily available to all, with special consideration for the prime target group: national and CIIP teams.

Critical Information Infrastructure Protection Initiative

This GFCE initiative will develop a CIIP Capacity Framework to identify a structure of capacities and to perform a stocktaking of good practices in order to inspire and stimulate the development and improvement of CIIP. CIIP is often difficult to grasp and this initiative will give concrete and actionable ways to policymakers to support. The initiative explained that a capacity framework on CIIP is highly needed because protecting information infrastructure is different from normal infrastructures. The information technology component is evolving rapidly, is intertwined with Critical Infrastructure, has global dependencies as well as diverse range of stakeholders (commercial, global, etc.), different cyber threat actors and different cyber threat vectors and is more focused on resilience compared to infrastructure protection.

Call for participation for both the CSIRT Maturity Framework initiative and the CIIP initiative; All partners and nations are invited to contribute. The feedback is highly valued and the initiative will strive to incorporate the feedback into the framework.

World Bank's Digital Development Partnership (DDP)

- **Ms. Sandra Sargent, Senior Operations Officer, Digital Development**
- **Mr. David Satola, Lead Counsel, Technology and Innovation at World Bank**

The World Bank made a presentation on its Digital Development Partnership (DDP) that helps operationalize the 2016 World Development Report on Digital Dividends and it offers a platform for digital innovation and development financing. The DDP brings public and private sector partners together to catalyze support to low- and middle-income countries in the articulation and implementation of digital development strategies and plans. This partnership makes digital solutions available to developing countries with an emphasis on the following areas: Data and Indicators, Digital Economy Enabling Environment, Cybersecurity, Internet Access for All, Digital Government, Mainstreaming Digital Services, Solutions, and Platforms.

In addition, a presentation on a toolkit of the WB called: Combatting Cybercrime, Tools and Capacity Building for Emerging Economies was conducted. The resources available are aimed at building capacity among policy-makers, legislators, public prosecutors & investigators, and civil society in developing countries in the policy, legal and criminal justice aspects of the enabling environment to combat cybercrime. These resources include:

- A Toolkit that synthesizes good international practice in combatting cybercrime;
- An Assessment Tool that enables countries to assess their current capacity to combat cybercrime and identify capacity-building priorities;
- A Virtual Library with materials provided by Project participating organizations and others.

Charter of Trust

- **Mr. Steffen Endler, Senior Vice President Siemens Singapore and Head of the Siemens Digitalization Hub**

The Charter of Trust (CoT) is a private-private initiative of 16 global multinationals (including GFCE Members Cisco and IBM) that started in 2018, addressing the risks following the growing exposure worldwide to malicious cyberattacks, putting the stability of society at risk. The CoT has three important objectives: to **Protect data** of individuals and companies, **Prevent damage** to people, companies and infrastructures and **Create a reliable foundation** on which confidence in a networking, digital world can take root and grow.

For this matter, CoT came up with 10 key principles that are taken forward by the signatories and underlined to the outside world. These principles and more information on the Charter of Trust can be found on the CoT website.

INTERPOL's Cyberspace and New Technologies Lab

- **Ms. Anita Hazenberg, Director of the INTERPOL Innovation Centre**
- **Mr. Theo van der Plas, Programme Director Digitalizing and Cybercrime, Police, the Netherlands**

This session elaborated on a recently developed initiative by INTERPOL and Netherlands Police on capacity building and test bedding for digital policing to combat emerging cyberspace threats.
In light of the increasing criminal use of Darknet and Cryptocurrencies the INTERPOL Innovation Centre (IC), with support of NL Police, set up the Cyberspace and New Technologies Lab (CNTL). Through its presentation, INTERPOL called upon the GFCE Community to support INTERPOL in its endeavor to deliver new, effective and affordable policing capabilities. This is accompanied by a global capacity building program for the 192 INTERPOL Member Countries.
Proposals are called on the identified priority working areas:

- Darknet and Cryptocurrencies analytic technologies;
- Training and capacity building solutions;
- Access to expertise and research capacity on Darknet and Cryptocurrencies;
- Resources to strengthen the Cyberspace lab. For example via donations and/or secondments of staff to the lab in Singapore as already undertaken by TNO (The Netherlands) and SECOM (Japan).

INTERPOL's ways of working envisaged through this call for participation:

- Cyber capacity building in close cooperation with operational teams in the INTERPOL Member Countries and members of the GFCE;
- Road mapping and testing capabilities to combat Dark Web crimes;
- Hosting and facilitating the Global Working Group on Darknet and Cryptocurrencies;
- Empowering effective partnerships with other international Law Enforcement organizations (such as Europol and CEPOL) and with partners from academia and industry.

Interested parties are invited to contact the Innovation Centre edgci-ic@interpol.int.

The Cyber Surakshit Bharat Program

- **Mr. Rakesh Maheshwari, Sr. Director Cyber Law & E-Security, Ministry of Electronics and Information Technology.**

This presentation conducted by Digital India, A Government of India Program, concerned a Cyber Security Capacity Building Program for Government CISOs through Public Private Collaboration. The

Cyber Surakshit Bharat (CSB) program is a public-private initiative to promote awareness and adoption of better Cyber Security practices in Government and Public Sector organizations.

The objective is to educate and enable Government officials (CISOs as well as frontline IT staff) with the latest on Cyber Security to ensure the security of all government e-infrastructure and services as well as citizen data available on the digital domain.

Target audiences are designated CISOs from all Central and State Government departments /Banks/ Defense. Deep Dive Cyber Security Trainings are given to a target of 1200 CISOs and Frontline Technical Officers in 2018 and in six cities (Delhi, Mumbai, Kolkata, Chennai, Hyderabad & Bengaluru).

Five programs have been conducted so far in various cities across the country. Seven more programs are planned up to February 2019. Future ambitions are to make the outreach of the program to a wide audience, to make use of Learning Management System (LMS) and to have regular revision of the content.

Cisco Networking Academy

- **Ms. Marcella O'Shea, Regional Manager ANZ & ASEAN, Corporate Affairs**

The Cisco Networking Academy is Cisco's largest CSR program. For 20 years, it is an IT skills and career-building program, developing the entry-level talent needed to power the digital economy.

Cisco partners with more than 11,000 learning institutions in 180+ countries to deliver the Networking Academy curriculum to over 1.87 million students each year.

Key to the program is the delivery of technical training and problem-solving experiences to individuals studying networking, security, and IoT technologies. As the demands of the workplace change, so does their program.

The Networking Academy Portfolio is categorized by learning outcomes and technology domain product lines. It has a range of instructor-led and self-paced courses that prepare students for entry-level jobs, career transitions, and professional certification. Students gain practical experience and practice troubleshooting in labs using real equipment and through digital simulation tools. A global network of support and training centres prepare local instructors to coach and mentor instructors to encourage innovative and entrepreneurial thinking.

Presentation GFCE Developments

- **GFCE Foundation**

GFCE co-chair of the Netherlands, **Ms. Carmen Gonsalves**, elaborated on the process and the importance of the establishment of a GFCE Foundation in the near future.

A GFCE Foundation allows to further strengthening the GFCE and particularly the work done by the Secretariat. As the work done by the GFCE community intensifies and focuses more on implementation, the GFCE Secretariat plays a central role in facilitating the community as its linking pin. In particular, the GFCE Secretariat will play a crucial role within the Working Groups.

Having a sustainable structure is essential for the GFCE to remain relevant for future challenges and to continue the important work in the field of cyber capacity building. The establishment of the GFCE Foundation implies that the GFCE becomes more flexible to receive and dedicate resources, expertise and knowledge. A GFCE Foundation will enable the GFCE to further internationalize. The establishment of a GFCE Foundation has no consequences for the current GFCE structure.

Further and on behalf of the Netherlands, Ms. Gonsalves stressed that the Netherlands will continue to support the GFCE (including the GFCE Secretariat) with resources (as it has done the past three years), and is looking forward to make this a joint effort with other members of the GFCE.

- **Internationalization of the GFCE Secretariat**

The Head of the GFCE Secretariat, **Mr. David van Duren**, continued with a presentation on the internationalization of the GFCE Secretariat.

He first stresses the importance of the GFCE foundation for the further development (internationalization, strengthening of capacity and sustainability) of the GFCE (including the GFCE Secretariat).

Additionally, Mr. Van Duren described that gradually the GFCE is shifting its focus from awareness to implementation. The steps that are taken by the GFCE community over the past three years describe this:

1. Building a strong personal network among GFCE members;
2. Broadening the amount of (action oriented) initiatives within the GFCE (raising awareness and sharing knowledge);
3. Creating an overview on CCB activities within the Cybersecurity Capacity Portal (in cooperation with the GCSCC);
4. Creating a common focus with the development of the Delhi Communiqué;
5. Formation and the kick-off of the five Working Groups along the line of the five themes of the Delhi Communiqué.

Finally, Mr. Van Duren made some announcements of members who are supporting/have committed to support the GFCE Secretariat:

- India: has appointed a GFCE regional liaison officer;
- UK / FCO: will appoint a GFCE Secondee per January 1st 2019.
- US: working with the OAS and its members to appoint a regional liaison officer for the GFCE.
  - Microsoft: provides Microsoft Teams (online working space) for the GFCE Working Groups and Secretariat.

Presentation of the Global Cyber Expertise Magazine #5

- **Ms. Alison August Treppel,** *Executive Secretary Inter-American Committee against Terrorism (CICTE), Organization of American States (OAS)*

The Global Cyber Expertise Magazine is jointly published by the African Union, the European Union, the Global Forum on Cyber Expertise and the Organization of American States and is produced bi-annually. As the representative of one of the Editors, Ms. Alison August Treppel presented its fifth edition during the GFCE Annual Meeting. The new version of the Magazine keeps you up-to-date on the latest CCB developments around the world.

All these cover stories, as well as many other articles, can be found in the physical as well as a new interactive online version of the Magazine, are **available online**.

DAY 2 – Thursday 20 September 2018

GFCE Annual Meeting: Opening Day 2

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

Mr. Secretary opened Day 2 of the GFCE Annual Meeting with a short recap of Day 1 and by providing an outline for Day 2. The focus of the first day of the GFCE Annual Meeting was to stress the need for cyber capacity building on a global level and the important role for the GFCE as a neutral, inclusive, action-oriented platform in this field. This was underlined in the opening's panel discussion as well as during the Roundtable sessions on the progress of the GFCE Working Groups and the presentation of the GFCE developments on the Foundation and the internationalization of the GFCE Secretariat.

The second day of the GFCE Annual Meeting kicked-off with panel discussions on linking both the CCB knowledge community (e.g. the development of the CCB knowledge portal) as well as CCB research to the GFCE community. The Annual Meeting participants had the opportunity to reflect in Roundtable sessions on the GFCE developments, and the GFCE Working Group Chairs presented their respective Working Group's progress in a short presentation.

Mr. Secretary underlined the uniqueness of the GFCE, and the Annual Meetings, which provide the opportunity to bring inspired people together to ensure that the GFCE remains and continues to develop as the platform for CCB cooperation at the cutting edge of innovation and inclusion.

Presentation of the CCB Knowledge Community

- **Mr. David van Duren, Head of the GFCE Secretariat**
- **Ms. Carolin Weisser, Lead International Operations, Global Cyber Security Capacity Centre (GCSCC)**
- **Mr. Bart Hogeveen, Head of Cyber Capacity Building, Australian Strategic Policy Institute (ASPI)**
- **Mr. Damir 'Gaus' Rajnovic, Chief Financial Officer (CFO), Forum of Incident Response and Security Teams (FIRST)**
- **Mr. Vladimir Radunović, Director of E-Diplomacy and Cybersecurity Educational and Training Programs, DiploFoundation**

The session entailed a panel discussion with representatives from the CCB Portal Advisory group who explained the importance of and need for (practical) knowledge sharing, the CCB knowledge portal, and connecting the CCB knowledge community to the GFCE community, and to the Working Groups in particular To this end, it is essential that there is a one-stop shop portal on CCB with relevant information for CCB implementation.

Some ideas that were discussed during the presentation:

- The content of the portal should be connected to the needs of the GFCE community, to assure the portal in line with the themes / topics of the Delhi Communiqué;
- Neutrality and global ownership of the CCB Knowledge Portal is important;
- Many portals already exist. Avoid duplication of efforts by making use of existing resources / information.

The way forward includes the following elements:

- Deliver a business plan by the 'CCB advisory portal group' (including the governance of content);
- Involve the GFCE Working Groups, Advisory Board and the GFCE community in the process;
- Finding financial support;
- Delivering a first version of the CCB Knowledge Portal in 2019.

Panel discussion Insights CCB Research

- **Moderator: Ms. Yurie Ito, Founder, Executive Director, CyberGreen**
- **Mr. Ian Wallace, Senior Fellow and Director of the Cybersecurity Initiative, New America**
- **Mr. Max Smeets, Postdoctoral Cybersecurity Fellow, CISAC, Stanford University**
- **Mr. Patryk Pawlak, Brussels Executive Officer, European Union Institute for Security Studies (EUISS)**

This panel demonstrates the significance of research on the topic of Cyber Capacity Building by presenting insights of their research. Studies on CCB are limited while the need for relevant scientific research is there. Moderated by Yurie Ito from CyberGreen, the panelists spoke about their research from their different perspectives (government research, academia) and then discussed the strengths and weaknesses of each approach in the context of capacity building.

Ian Wallace presented a mini case-study on the role of think tanks in cybersecurity capacity-building: the case of cybersecurity & international development'. He set out the role that think tanks can play in the work of the GFCE using New America's Securing Digital Dividends paper.

This was followed by Patryk Pawlak sharing his insights from a recent study by EUISS named Operational Guidance for the EU's international cooperation on cyber capacity building. This extensive study provides a comprehensive practical framework when designing and implementing the EU's external actions against cybercrime and for promoting cybersecurity and cyber resilience. The Operational Guidance is accompanied by a Playbook – an actionable summary that provides a quick overview of the main steps to follow and key challenges to take into consideration when designing and implementing cyber capacity-building interventions.

Finally, Max Smeets elaborated on his recent paper entitled *Determinants of Cyber Readiness* written together with Christos Makridis, a digital fellow at the MIT Sloan Initiative. The paper examines why some countries have a higher (measured) level of 'cyber readiness' compared to others. The study shows e.g. that countries facing a more threatening security environment or which are highly dependent on cyberspace are more likely to have a high level of cyber readiness. The study also showed that a country's level of ICT exports is one of the most robust and important predictors of cyber readiness.

Roundtable discussions 2: GFCE – Next Steps

The roundtable discussion on Day 2 focused on the GFCE developments. During this interactive session, the GFCE community was given the opportunity to give feedback on the plans and how they foresee the GFCE's next steps. Therefore, the aim of this session was to collect thoughts and ideas from the GFCE Members and Partners on the latest GFCE developments as the Foundation and the internationalization of the GFCE Secretariat.

The roundtable session resulted in new ideas and comments on the GFCE developments, which will be shared with the GFCE community and discussed with the GFCE co-chairs, the Advisory Board and the GFCE Secretariat in the coming weeks. Kindly find a short overview of the main elements mentioned below:

- The **clearing house function** within the Working Groups was mentioned several times as the development within the GFCE that has a lot of potential. The advice from the GFCE community in the roundtable session was to formalize the process, and to make it crosscutting in the Working Groups for a harmonized and transparent process.
- There were enthusiastic reactions to the announcement of the **GFCE regional liaisons**. This creates the opportunity to increase involvement of regional stakeholders within the GFCE.
- The **GFCE Foundation** creates possibilities to increase the number of funding Members in the GFCE and will create a channel for fundraising.

Presentation GFCE Working Groups – Progress reports by WG Chairs

The Chairs of the Working Groups presented the progress of their respective Working Groups.

Working Group A - Cyber Security Policy and Strategy

- **Mr. Chris Painter**, Chair of Working Group A - Cyber Security Policy and Strategy

The theme Cyber Security Policy and Strategy can be seen as the foundation of the other identified themes in the Delhi Communiqué. A National Cybersecurity Strategy is the first step to tackle other cyber issues. Therefore, the Working Group aims to help countries and other stakeholders improve their policy and strategy making capacity. The ultimate goal of Working Group A on Cyber Security Policy and Strategy is to actively reach out to countries who are missing a NCS and play matchmaker by connecting resources with needs. A great first example of this is the request that was made by Tunisia and how it is being picked up by various stakeholders of the working group.

Working Group B - Cyber Incident Management and Critical Information Protection

- **Mr. Abdul-Hakeem Ajijola,** Chair of Working Group B - Cyber Incident Management and Critical Information Protection
- **Mr. Maarten van Horenbeeck**, Task Force leader of Cyber Incident Management
- **Mr. Marc Henauer**, Task Force leader of Critical Information Protection

This WG has defined four high level goals comprising of 1) Identifying obstacles and carrying out gap analysis, 2) Collecting maturity metrics 3) Developing a repository of Good Practices and 4) Develop recommendations. The two topics have been divided and appointed to two taskforce leaders and each one of them have defined objectives. The Task Force Cyber Incident Management focuses on the Lessons Learned from capacity building projects and will make a CSIRT Maturity Framework globally available, with funding from the Netherlands. The task force CIIP will focus on the fundamentals of CII, stakeholder management in the field of CII and the effect of the supply chain to CII. Both taskforces will incorporate exercises in their objectives. The Working Group has set itself a strong timeline and has an energetic focus.

Working Group C – Cybercrime

- **Mr. Zahid Jamil,** Chair of Working Group C – Cybercrime

The WG agreed to deliver an outcome document by the end of 2018 that is the synthesis of a mapping exercise of the various CCB efforts in the area of Cybercrime and its analysis for identifying best practices (as detailed below). It was agreed that the Secretariat should conduct calls with actors to collect information, in addition to seeking responses to the format developed.
Collate within the outcome document this information and conduct therein:

a) a mapping of the various ongoing projects being conducted by the various cybercrime CCB actors surveyed;
b) based upon the mapping exercise cross reference ongoing projects in different areas and regions;
c) and based upon the mapping exercise analysis that provides (not a framework) but identifies elements of best practice to be listed for guidance;

The Cybercrime Working Group by 2019:

a) Awareness raising of internationally recognized best practices on legal frameworks, such as the Budapest Convention.
b) Sensitize donors towards quality and not just quantity – a best practice to measure.
c) Identify gaps in cybercrime CCB at the global level with the aim of facilitating the filling of these gaps.

d) WG should aim for fostering regional cooperation i.e. countries with common aspects and similarities e.g. South – South.
e) WG should aim for long-term commitment in its initiatives with the aim of building a good understanding of the different contexts and reflecting that in the group's different functions.

Working Group D – Cyber Security Culture and Skills

- **Mr. Vladimir Radunović**, Chair of Working Group D - Cyber Security Culture and Skills

Working Group D on Cybersecurity Culture and Skills defined the following way forward for both Task Forces: (1) Mapping of existing campaigns and programs, and (2) Overview of the gaps and needs in all countries.

On the topic of Cybersecurity Awareness the way forward is: (1) Mapping of existing awareness campaigns, (2) outreach GFCE community, (3) White paper with criteria for awareness raising campaigns with lessons learnt from other policy areas, such as public health campaigns. Actionable: GFCE Cyber Security Awareness in October. On the topic of Cybersecurity Education and Training: (1) Mapping of existing education and training programs, (2) Mapping of skills and competences needed, starting from existing corporate templates, (3) Defining needs of beneficiaries, (4) Parameters for mapping: consider scalability of existing training. Actionable: GFCE Academy with aggregate on available courses within the GFCE community.

Important aspects are metrics, sustainability and commitment GFCE community, quick results and cultural context (language).

Working Group E – Cyber Security Standards

- **Mr. Andrei Robachevsky**, Chair of Working Group E - Cyber Security Standards

The role of the Working Group is functioning **as a clearing house**. Therefore, for instance a repository of various initiatives can help **raise awareness, avoid duplication of efforts and enable collaboration**.

The focus of the Working Group is on two topics:

1) Internet Of Things (IOT): an emerging and urgent area. The goal is to promote relevant IoT security standards and practices by providing real-life case studies of successful deployments. Make use of what there already is among GFCE members and other relevant organizations. Another point that was brought up was that **IoT might be a topic too broad** already. One of the ideas was to start with industrial IoT, as a more "organized" area.
2) Open Internet Standards (OIS). This is the foundation of the internet. More focus is needed on deployment. The Working Group is taking the approach of facilitating deployment by displaying successful deployment initiatives (e.g. triple I initiative) and tools (e.g. internet.nl).

A form that could be used for Working Group E is webinars or meetings were relevant parties are brought together. Key elements: e.g. existing frameworks / approaches of countries (including applicable compliance frameworks), lessons learned.

Closing remarks

- **Mr. Teo Chin Hock, Deputy Chief Executive (Development), Cyber Security Agency Singapore**

The theme for this year's SICW is *Forging a Trusted and Open Cyberspace*. In this regard, it is apparent that the work of the GFCE is both significant and extremely relevant. As a coordinating platform, the GFCE encourages dialogue among multiple stakeholders on how best to implement cyber capacity building measures. These capacity building measures are crucial in building confidence and trust among like-minded partners.

Singapore was privileged to host the 3rd GFCE Annual Meeting and stands ready to support the GFCE through the ASEAN-Singapore Cybersecurity Centre of Excellence. The new Centre will be expanding on the existing ASEAN Cyber Capacity Program's task of building regional capacity in a multi-disciplinary and multi-stakeholder manner, covering the areas of *cybersecurity strategy*, *legislation and norms* as well as *technical and operational expertise*. It will thus be beneficial for GFCE members to work in tandem and leverage on existing efforts such as these in order to yield better returns on our investments.

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

Ms. Gonsalves started thanking the Cyber Security Agency Singapore (CSA) and specifically Mr. Teo Chin Hock, for their tremendous efforts and kind hospitality in hosting this 3rd GFCE Annual Meeting. In that sense Mr. Teo's final remarks are illustrative of Singapore's much appreciated contribution to CCB in the ASEAN region as well as to the GFCE.

Furthermore, Ms. Gonsalves expressed her gratitude and thanks to her co-chair, Mr. Ajay Sahwney, for the support and efforts on global cyber capacity building made by India. The cooperation as co-chairs certainly demonstrates a communality of purpose, based on a shared commitment. In addition, the GFCE members were thanked for their active participation in the Annual Meeting and especially within the Working Groups. The GFCE members are the heart of the GFCE and we all are looking forward to the activities and outcomes of the Working Groups in the coming year.

Finally, the GFCE calls for expressions of interest to host the next Annual Meeting. Please reach out to the GFCE Secretariat for further information.

The GFCE secretariat wishes to thank all participants for their valuable contributions to the GFCE Annual Meeting 2018 and we look forward to our continued close cooperation.