Report GFCE Annual Meeting 2016 in Washington D.C.

June 2016

Executive summary

Over 100 cyber policymakers and stakeholders attended the first GFCE Annual Meeting on 1 and 2 June in Washington D.C. In 16 different workshop sessions 41 GFCE member and guest speakers presented initial outcomes of their cyber capacity initiatives and projects.

The Economic Community of West African States (ECOWAS) and Peru were welcomed as new members which brings the total GFCE membership to 52. A new initiative by Japan and the United Kingdom was launched to help CERTs remedy risks in order to achieve a more sustainable, secure and resilient cyber ecosystem (CyberGreen). Two pitches for new initiatives were launched by the Bank of England (CBEST) and the European Union (Research Initiative).

A new GFCE Advisory Board was installed consisting of 10 members from civil society, academia and the tech community who will advise GFCE members on strategy and implementation of initiatives.

During the Annual Meeting also organizations and experts from outside the GFCE community presented their experiences on cyber capacity building. In his key note speech Mr. Fadi Chehadé, Senior Advisor to the Chairman of the World Economic Forum provided an overview of developments that will shape the future of the digital economy and society. A number of best practices were presented by the Potomac Institute, DiploFoundation, Huawei and the Estonian Ministry of Foreign Affairs. The European Union and the Council of Europe provided an overview of their Global Action on Cybercrime (GLACY) to support countries in implementation of the Budapest Convention on Cybercrime.

During a plenary session the Strategy for 2016 and 2017 was discussed. This strategy will be finalized in the coming months and positions the GFCE as the global platform for cyber policymakers and stakeholders to coordinate and implement cyber capacity building.

Finally the Global Cyber Expertise Magazine was launched, the new tri-annual magazine on global cyber capacity building by the AU, EU, GFCE and the OAS.

Proposed actions

Actions	Deadline
Comments by members & Advisory Board on Strategy	16th September 2016
Final draft Strategy provided by co-chair	1st October 2016
Comments final draft Strategy (silent procedure)	1st November2016
Expression of interest Research Initiative	1st August 2016
Expression of interest CBEST pitch	1st August 2016
Submissions/articles Global Cyber Expertise Magazine	31st August 2016
Candidate host next Annual Meeting	16th September
Candidates GFCE Co-Chair	1st October 2016

Contents

DAY 1

Welcome and Opening Speeches

Mr. Francisco Lainez (Senior Security Advisor OAS) welcomes the participants to OAS and outlines OAS involvement in cyber capacity building. Within the GFCE the OAS is working on a number of cyber capacity building initiatives, such as conducting cybersecurity assessments in all countries in the LAC region.

Mr. Christopher Painter (Coordinator for Cyber Issues at the US Department of State) argues for the importance of building international consensus on the direction of cyber capacity building and to work together to overcome some of the challenges in the cyber policy field.

Prof. Uri Rosenthal (Special Envoy Cyber of the Kingdom of the Netherlands) provides an overview of the context of the establishment of the GFCE, the work done in the last year and the challenges ahead. He reaffirms the multistakeholder approach of the GFCE and the mission statement stressing a cyberspace that is free, open and secure. He reiterates that cyber is a global issue and localized vulnerabilities have global consequences. GFCE can act as a 'linking pin' for global coordination and collaboration.

New CyberGreen Initiative & Advisory Board

Ms. Matsuzawa (Japan) elaborates on the purpose of the CyberGreen initiative which is to offer a novel methodology to understand and assess the health of the cyber ecosystem.

Wouter Jurgens (Chair GFCE) expands on the successes of the GFCE initiatives over the past year and attendance at global conferences. This Board consists of 10 members from civil society, academia and the tech community who will advise GFCE members on strategy and implementation of initiatives. Reiterates Mr. Rosenthal's welcome of the Advisory Board and reaffirms the mission statement of the Advisory Board. The Advisory Board He gives a short explanation of the selection procedure of the Advisory Board members.

Mr. Yedaly (co-chair Advisory Board) thanks the panelists and elaborates on the gender and regional balance of the Advisory Board.

Wouter Jurgens (Chair GFCE) explains why the appointment of the second GFCE co-chair has been delayed to provide an opportunity to the next host of the Global Conference on CyberSpace to become GFCE co-chair.

BREAKOUT 1

Coordinated Vulnerability Disclosure (CVD)

Mr. De Vries (Head of National Cyber Security Centre, The Netherlands) explains the Dutch model of cyber security, specifically the integration of public-private partnerships. He stresses the role of the government as being a facilitator and promoter due to compatibility issue with respect to different legal and cultural backgrounds. He argues that establishing guidelines as opposed to laws is more effective, sidestepping oversight issues. He elaborated on the Coordinated Vulnerability Disclosure Manifesto in which organizations commit themselves to implement Coordinated Vulnerability Disclosure.

Mr. Corman (I am The Cavalry) expands on the new term chosen 'coordinated vulnerability disclosure' vs 'responsible disclosure'. He highlights four elements required for a coordinated vulnerable disclosure: brand promise, initial program and scope, we-will-not-take-legal-action-if, coordinated mechanism and expectation. He elaborates on the practical vulnerabilities from the internet of things. He further argues that we are approaching a tipping point in public awareness with respect to consequences of a cyber-attack and we are in need of a change in cyber culture.

Ms. Tóth (Ministry of Foreign Affairs, Hungary) & **Ms. Popescu** (Ministry of Foreign Affairs, Romania) provide an explanation on their nations programs on CVD. They announce a next Coordinated Vulnerability Disclosure Expert Meeting in November 2016 in Rumania to which all GFCE members will be invited.

Assessing and developing cyber capability

Lara Pace (director of Strategy and External Engagement, GCSCC) elaborates on the Cyber Maturity Model (CMM) and how it has proven to be successful for many countries worldwide. The CMM provides countries or regions with a comprehensive analysis of their cybersecurity capacity. Such a strategy is important for countries to set out their national priorities in cyber. Since cybersecurity capacity is increasingly important as a factor in foreign direct investment the GCSCC encourages countries to share their CMM report where possible.
For the future GCSCC is aiming for continued deployment of the CMM via regional centers. A first regional center has already been launched in Australia. GCSCC is continuously working on the further development of CMM and of complementary models like the Cyber Harm Model and CMM for organizations.

A good example of the use of CMM is presented by **Belisario Contreras** (Cybersecurity Program Manager, Organization of American States) who shares the outcomes of the 2016 Cybersecurity report: 'Are we Ready in Latin America and the Caribbean?' This report was developed in close cooperation with IDB, the Potomac Institute and Microsoft.

Robert Collett (head of Capacity Building, Prosperity and Cyber Crime, UK Foreign Office) briefly spoke about the UK position regarding cyber capacity building and their partnerships on this topic with over 70 countries.

BREAKOUT 2 & 3: inspiring examples of non-GFCE initiatives

National Cyber Security Index (NCSI 1.0)

Ms. Helen Popp (ministry of foreign affairs, Estonia) announces a new cyber security assessment tool NCSI 1.0 developed by Estonia which was launched just days ago. She argues for the need to have a baseline cyber security management and military defense. The NCSI measures countries' preparedness to prevent the realization of cyber threats and readiness to manage cyber incidents, crimes and large-scale cyber crisis. In other words, the NCSI is a global index, a global database and a tool for cyber security capacity building. In the presentation Ms. Popp elaborates on the methodology of the NCSI 1.0 and refers to the website for further information (http://www.ega.ee/)

Supply Chain Risk

Mr. Donald Purdy (CSO Huawei) outlines the concept of supply chain risk and stresses the importance of international collaboration. International collaboration is essential because:

- Networks and systems are vulnerable to attacks.
- Agreement on standards/best practices/norms of conduct is needed.
- ICT products are vulnerable
- Country-specific regulations can equal trade barriers
- Conflicting buyer-specific requirements causes inefficiency (costly for ICT providers)

Global Action on Cybercrime (GLACY)

Mr. Pereira (Project Manager GLACY Program, Council of Europe) and **Ms. Barmpaliou** (Program Manager, Organized Crime and Cybersecurity, EU Commission, DG International Cooperation & Development) elaborate on the Global Action on Cybercrime (GLACY) project. This project provides resources to support States to implement the Budapest Convention on Cybercrime. GLACY currently has 49 Members (State Parties), 17 observer States and 12 organizations (e.g. African Union Commission, European Union, OAS, Interpol, UNODC, ITU). Focus of GLACY is on strategies, harmonization of legislation, judicial training, law enforcement capacities and international cooperation. Soon GLACY+ is about to be to be launched: Global Action on Cybercrime Extended; 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.

Cyber readiness index

Ms. Hathaway (senior fellow Potomac Institute) elaborates on the fundamental dependencies of the global economy on the internet and highlights the risks inherent in digital economic development.
In her presentation Ms. Hathaway lists applications of internet services, stating that the anticipated GDP growth of connecting Citizens to the Internet is +4% to 10%. But on the other hand the Economic Opportunity of the Internet is at risk (due to activism, fraud, espionage, and other destructive activities). Therefore it is important to measure and assess cybersecurity. The Cyber Readiness Index 2.0 is a comprehensive, comparative, experience-based methodology to evaluate a country's maturity and commitment to securing their national cyber infrastructure and services upon which their digital future and growth depend.

Building Cybersecurity Competences

Mr. Vladimir Radunovic (Director E-diplomacy and Cybersecurity Programs at the DiploFoundation) presents key findings from the report 'Cybersecurity Competence Building Trends – Policy options from OECD countries'. The report consists of a review of trends and policy instruments of 10 OECD countries on cyber competence building (Estonia, Israel, Republic of Korea, the Netherlands, UK, US, Austria, Finland, France and Germany).
Key findings of the study:

- Countries observe both risks and opportunities: cyber preparedness and global industry competitiveness;
- A combination of long-term and short-term approaches is necessary to transform labor markets;
- PPP involvement (development of curricula, certification, capabilities, regional hubs):
    1. Strategic lead and incentives by the government;
    2. Funds and cutting-edge technology by the private sector;
    3. Knowledge, outreach and research potential by academia.

BREAKOUT 4

Internet Infrastructure Initiative

Mr. Bart Hogeveen (Clingendael Institute, Netherlands) and **Dr. Joanna Swiatkowska** (The Kosciuszko Institute) state that it is vital for consumer trust that users can rely on fundamental internet protocols and internet standards functioning properly. There are sufficient internet standards but implementation is lacking behind. This initiative is about ways to speed up implementation of standards, through expanding existing practices and exploring new solutions and ways of cooperation. A practical deliverable of this initiative is the website internet.nl, a tool to test if a website complies with existing internet standards. Also the initiative helps other parties, like Poland to develop Cybersectest.el a Polish version of the internet.nl.

Global Campaign to raise cybersecurity awareness

Ms. LaHaie (US Department of State), **Ms. Siegel** (US Department of Homeland Security) and **Mr. Contreras** (Organization of American States) present the cybersecurity awareness initiative. The U.S., Canada and OAS work closely together in promoting cyber awareness to the general public.

Recent progress of the coalition:

- Cooperation and alignment between Stop.Think.Connect, GetCyberSafe and other existing cybersecurity awareness campaigns.
- Joint promotion of culturally specific cyber safety resources.
- Coordination of cyber-focused events either in-person or via social media.
- In their coordinated efforts, the U.S., Canada and OAS encourage global adoption of October as Cyber Awareness Month.

BREAKOUT 5

Critical Information Infrastructure Protection (CIIP) Initiative

Mr. Mor Sola (Spain) outlines the Critical Information Infrastructure Protection (CIIP) initiative. This initiative creates opportunities for the Meridian Community to assist and partner with developing countries and organizations to help improve CIIP globally.

The initiative offers training to CIIP policy makers (with a focus on developing countries) en marge of the Meridian conference November 2016 in Mexico.

The initiative has 3 components:

1. Primer Day to the Meridian Conference with the following program: Presentations on CIIP concepts and terminology; an overview of the main international organizations; a highly interactive ‘problem clinic’ with experts helping to answer questions;
2. A research project aiming to analyze the state of CIIP across the world (up to 200 countries).
3. A buddying system in which CIIP experienced countries from the Meridian community are matched with countries which want to develop CIIP capacity.

Promoting Cybersecurity Due Diligence across Africa

Mr. Lord and **Mrs. Bills** of the Software Engineering Institute and **Mr. Hodgson** of MITRE elaborate on promoting Cybersecurity Due Diligence across Africa. The highlight key aspects regarding ‘Capacity Development Implementation’:

- Promoting and collaborating with local experts: local experts provide critical insights to shape initiatives. They often have a track record of success in related areas and they are able to connect with relevant stakeholders.

- Fostering regional cooperation: Technical exchanges between cybersecurity practitioners create a medium for regional working groups and initiatives, which enable regional leaders to lead.
- Facilitating Mentorship of National CSIRT's.

BREAKOUT 6

Preventing and combating cybercrime in South East Asia

Ms. Matsuzawa (Japan) elaborates that Japan will actively engage in capacity building based on its experience in ICT development. Elements of the initiative to prevent and combat cybercrime in South East Asia are:

- Promotion of the Budapest Convention on Cybercrime to encourage more countries in South East Asia to sign up;
- training to foreign police officers;
- training to foreign criminal justice specialist.

Mr. Neil Walsh (UNODC), elaborates on the United Nations Global Programme on Cybercrime. The program builds a cross-government response with the following elements: Diplomacy, Policy, Law Enforcement, Prosecution / Judgment & National Prevention. Results include:

- Regional basic and advanced training to prosecutors, investigators and CERTs on electronic evidence extraction, investigation and prosecution of cybercriminals) .
- National coordination and public/private partnership workshops on cybercrime in Myanmar, Thailand, Viet Nam, Philippines and Cambodia. Attendees included law enforcement, judges, prosecutors, CSPs & ISPs, banking and national experts.
- Country assessment reports

Cybersecurity and cybercrime trends in Africa

Mr. Bill Wright (Symantec Corporation) and **Mr. Moctar Yedaly** (African Union Commission) elaborate on the soon-to-be published report that collects and presents detailed technical data on cybersecurity threats and trends in Africa in partnership with African thought-leaders. The study assesses the major trends in the African region in terms of threats to the cyber domain and the potential impact they could have on internet users. Through voluntary country surveys, the report takes stock of the advances in policy and legal frameworks that government authorities have instituted in order to better address the challenges that they face in an increasingly connected world.

BREAKOUT 7

CyberGreen

Ms. Yurie Ito (director CyberGreen) outlines the new CyberGreen initiative which has been taken up by Japan and UK. The initiative supports CSIRTs worldwide with metrics to measure the health of cyber eco systems. She stresses the need for a common understanding of cyber health and risks through a widely accepted way of measuring national, service provider, and enterprise cyber health and risks. A common understanding and insight will enable global policy development and capacity building. CyberGreen is different from other assessments because rather than study the vulnerabilities of a system it quantifies the threat an unsecure system poses to others.

Cybersecurity Initiatives in OAS member states

Ms. Kerry-Ann Barrett (Organization of American States) elaborates on the OAS activities in member states. Their focus is on 5 issues:

1. Development of National Cybersecurity Strategies;
2. Technical training (workshops and country-specific Technical Missions);
3. Cybersecurity exercises;
4. Development of national CSIRTs and a regional CSIRT Hemispheric Network and
5. Awareness raising, research and expertise.

Launch Global Cyber Expertise Magazine

Mr. Anne Blanksma Çeta of the GFCE Secretariat launches the new Global Cyber Expertise Magazine, a new magazine on global cyber capacity building jointly published by AU, EU, GFCE and OAS. The Magazine is available both in printed version and can be downloaded from the GFCE website. All members are encouraged to contact the editorial board with story ideas about relevant policy developments and initiatives. Members are also asked to distribute the online magazine via their network (via the GFCE website it is possible to subscribe to online magazine).

DAY 2

Key note speech: shaping the Future of the Digital Economy and Society

In his key note speech Mr. Fadi Chehadé, Senior Advisor to the Chairman of the World Economic Forum provides an overview of developments that will shape the future of the digital economy and society. He memorizes the historical decision by the US to let go of the ownership of ICANN. Development of the internet is and will be shaped by networks and will be organized bottom up. That is why the multistakeholder approach is important. He announces the launch by WEF of a platform for the development of cyber policy to stimulate growth of the cyber domain. This provides an opportunity to collaboration with the GFCE in the future.

BREAKOUT 8

Progressing Cybersecurity in Senegal and West-Africa

Ms. Lara Pace (Global Cyber Security Capacity Centre, University of Oxford), **Ms. Petra Nijenhuis-Timmers** (Ministry of Foreign Affairs, the Netherlands) and **Ms. Fatou Coundoul Thiam** (Ministere des Postes et des Telecommunications, Senegal) elaborate on the country review on the state of cybersecurity in Senegal. The resulting review report identifies 69 recommendations across 5 dimensions of cybersecurity capacity:

- Cyber Security Policy and Strategy;
- Cyber Culture and Society;
- Cybersecurity Education, Training and Skills;
- Legal and Regulatory Frameworks and
- Standards, organizations, and technologies.

As outcome of a GFCE Expert Meeting on Cybersecurity in West Africa in April 2016 Senegal and the Netherlands are currently working on the Dakar Declaration on Cybersecurity.

CSIRT Maturity

Mr. De Vries (Head of National Cyber Security Centre of the Netherlands) stresses that the topic of CSIRT Maturity is gaining importance. Several organizations (ENISA, FIRST, CyberGreen, TF-CSIRT, GFCE) work together on complementary areas in CSIRT maturity. One of the goals of the CSIRT maturity initiative within the GFCE is to cooperate with the various initiatives and to align the efforts that are under taken, to avoid duplications.

A result is a CSIRT maturity toolkit. This is a best practice document written by experts in the field, referencing well-established practices in the community. Mr. De Vries concludes with lessons learnt on CSIRT maturity:

- Building a CSIRT takes time.
- An established CSIRT has a responsibility to help the community (for example: set up CSIRTs, share materials, enable development, and introduce CSIRTs in the community).

Mr. Betz (Microsoft) elaborates on different CSIRT categories. He also presents some figures which indicate that the infection rate of is increasing. Examples of malware categories are: trojans, exploits, backdoors, ransomware, viruses, password stealers, etc. Microsoft keeps malware statistics per country on: www.Microsoft.com/SIR

Mr. Diego Subero (Cybersecurity Consultant, Organization of American States) talks about the efforts within the American States to build up CSIRTs. The OAS has developed a guide that can help with the implementation of a CSIRT (http://ow.ly/10Bhng). He elaborates on a technical CSIRT platform that is set up for the American States (www.csirtAmericas.org). It is a virtual community providing several services to help CSIRTs.

Opportunities for new GFCE Initiatives

Global Current State of Cyber Capacity Building

Ms. Carolin Weisser (Global Cyber Security Capacity Centre) gives a presentation on the GFCE portal (part of the website of the GCSCC www.sbs.ox.ac.uk/cybersecurity-capacity). The portal consists of over 100 cyber capacity initiatives worldwide. The database provides valuable insight on the following questions:

- What are the regional and global priorities with respect to capacity building?
- Where are the overlaps? And what are the differences between the regions?
- Are there any blind spots? And where are they?

At this point 3 sorts of initiatives/programmes can be distinguished within the portal:

- Global programmes
- Global programmes with regional focus / adaption in one or more region.
- National programmes in a bilateral or multilateral framework.

Trends and Developments in Global Cyber Capacity Building

A panel of GFCE members discusses about the future of global cyber capacity building.

- **Mr. Borrett (IBM)** explains the new concept of cognitive security. In the future cybersecurity systems will be increasingly able to understand, reason and learn. The concept is based on big data analysis to make sense of unstructured data. IBM is coordinating with 8 different universities to build a cognitive security system.

- **Mr. Yedaly (AUC)** outlines the lack of real understanding of the impact of cyber and cybersecurity, particularly among African political leadership. Raising awareness of cyber among political leaders and policymakers is therefore very important to successfully build cyber capacity.
- **Mr. Purdy (Huawei)** stresses the importance of having assessments to determine long term strategy. He argues for the necessity of global standards to ensure that non-legitimate software does not pose a security risk. There is a clear need for a paradigm shift with respect to law enforcement from reactive to proactive.
- **Mr. Dukes (US)** stresses that over the past decade cyber has become an increasingly pertinent topic for diplomats. Training of diplomats in cyber issues is crucial for productive engagement with other nations. Cyber has become the first area of interaction with other nations and thus is an integral part of the diplomatic dialogue. Also it extends far beyond the scope of government, making a multi-stakeholder approach a necessity.
- **Bill wright (Symantec)** outlines that cross-sector integration of cyber has great economic benefits but simultaneously presents huge challenges in increased vulnerability to cyber threats, both in terms of attack surface and attack vectors. The private sector owns the majority of ICT infrastructure and technology, has most expertise on cyber issues and is the motor for technological innovation. No government can therefor afford to take on cyber issues alone; coordination and cooperation is essential.

Outcomes GFCE Member Survey

Mr. Van Duren (Head GFCE Secretariat) reflects on the results of the member survey. The survey is mainly about getting more insight in (potential) initiatives. Mr. Van Duren starts with some general reflections. At this moment the GFCE consists of 12 initiatives. These initiatives can be divided in to 2 groups:

1. Global initiatives: could be of interest of all members and mostly they are about a specific topic (like CSIRT maturity or Critical Information Infrastructure Protection).
2. Regional initiatives: one or more members are committed to help a specific region (like for example South East Asia, Africa or the Americas). The initiative mostly has a broad scope, meaning that they include a broad program with several topics.

Key findings from the survey are that:

- Cybersecurity and cybercrime are seen as having the most priority by the GFCE members.
- Within the theme of cyber security we have members looking for expertise as well as offering expertise. This means there are opportunities within the GFCE for more initiatives.
- The majority of the GFCE members see data protection and e-governance having the least priority. The GFCE doesn't have initiatives on Data protection and E-governance yet. One in four of all members see e-governance and data protection as their first or second priority.

GFCE Strategy

Wouter Jurgens (GFCE Chair) highlights the most relevant topics of the strategy document. After this presentation the Chair asks the members to respond to the document.

Council of Europe agrees with the structure and scope of the GFCE strategy. Raises 2 issues on the first page: 1) spelling correction; 2) proposes different wording at P1 bottom paragraph ‘the GFCE is a unique platform to facilitate and strengthen capacity building efforts’.

South Korea thanks the GFCE Secretariat for preparation. Comments that the GFCE strategy is aimed at 2016-2017 while the long term goals go well beyond the 2017 context. Further proposing that items 4 and 5 can be integrated into item 3.

United Kingdom expresses support and endorsement of the strategy and the desire to assess the interest of members to set collective goals to further concretize the GFCE goals. Proposes a longer preparatory period to arrange potential meetings for the next GFCE meeting.

European Commission echoes the desire for more specific and concrete goals that support progress. Highlights the importance of linking the results of the initiative with setting of a global agenda. Would like to see that operational components are further translated to policy setting.

Canada stresses the amount of progress which has been made in the first year and congratulates on the successes. Recognizes that the agenda is ambitious and that some of the objectives are more long term. Highlights the convening power of the GFCE as one of the strongest points and that it is essential that the GFCE remain flexible to rapidly adjust to changes. Stresses the added value of a platform to put a spotlight on initiatives results.

Japan emphasizes the importance of the GFCE portal (executed by the GCSCC).

USA underlines the role of members to ensure that we are efficiently and effectively using the GFCE as a platform for participation. In particular, to maintain the necessary level of diversity in the work that the GFCE is doing.

Advisory Board (Radunovic) reaffirms the importance of the non-government actors as implementers in GFCE initiatives. The GFCE Advisory Board will be further discussing the strategy in the coming weeks and months. Underlines that having an Advisory Board is not an end in- and of - itself but rather the means to an end.

GFCE Chair concludes the meeting and invites members to provide written feedback on the GFCE strategy. Promises to present a timeline for further discussion on the GFCE strategy.

PITCHES

CBEST

Andrew Huddart (Bank of England) elaborates on CBEST, which is a framework to deliver intelligence-led cyber security tests. CBEST differs from other security testing currently undertaken by the financial services sector because it is threat intelligence based, is less constrained and focuses on the more sophisticated and persistent attacks on critical systems and essential services. CBEST provides a holistic assessment of financial services or infrastructure provider's cyber capabilities by testing people, processes and technology in a single test. The Bank of England invites GFCE Members to explore possible cooperation in a new GFCE initiative.

Research Initiative

Ms. Nayia Barmpaliou (EU Commission, DG International Cooperation & Development) presents a pitch regarding research capacity to strengthen expertise within the GFCE community. She describes 3 pillars:

1. general research on cyber capacity building (methodology, policy coherence, lessons learnt, recommendations);
2. research related to needs of GFCE initiatives;
3. research regarding blind spots within the field of cyber capacity building.