Report International kickoff meeting 2 & 3 November 2015

GFCE secretariat

12 November 2015

Executive summary

On 2-3 November the Netherlands hosted the international GFCE Kick off meeting in The Hague. 77 participants were welcomed at the meeting, 66 of them representing 38 GFCE members, 11 of them representing 9 partner organizations.

The **formal opening** was done by mr Uri Rosenthal, former Dutch Minister of Foreign Affairs and Special Envoy for International Cyber Policy, after which the participants were presented the mains goals of the meeting:

- To agree on the GFCE organisation and structure for 2015 and 2016

- To present an overview of the current GFCE initiatives and pitches for potential GFCE initiatives

- To network with other GFCE members and experts

- To obtain familiarity with the GFCE Secretariat and what it could do for you

GFCE organization and structure

On the second day members discussed the GFCE organization and structure referring to the draft Terms of Reference (ToR).

The following issues were discussed:

- **Terms of Reference GFCE Organization and Structure**. The initial response to the draft ToR was in general positive; no major objections were put forward by the members.

  Point of action: Members are invited to provide the Secretariat (at contact@thegfce.com) with written comments on the draft ToR by 30th November 2015.

  The Secretariat will circulate the final ToR with members by 15th December 2015.

- **Chair and Co-Chair:** The GFCE consists of a Chair, a Co-Chair, the GFCE Members and the GFCE Secretariat. Partners can participate in initiatives; The Netherlands will be Chair for the next coming four years; it is proposed to install a Co-Chair, this is renewable every four years. Aim is to balance the Chair geographically.

  Point of action: Members are invited to express their interest in Co-Chairmanship to the Secretariat (at contact@thegfce.com) before the 1st of February 2016.

- **New membership -** Applications for new membership will be evaluated based on their merit and proposed initiatives and will be considered by the members at the next annual meeting or if necessary in consultation by the co-chairs with the GFCE focal points.

- **Advisory Board** - It was proposed to install an Advisory Board consisting of representatives of civil society, tech community and think tanks to advice the GFCE on the involvement of partners.

  Points of action:

- A proposed Terms of Reference for the Advisory Board will be shared with the members by 1st of February 2016.
- Members are requested to share their written comments on the proposed ToR for the Advisory Board by 15th February 2016.
- Members are requested to share potential candidates for the board by 15th February 2016 (at contact@thegfce.com).

- I**nitiatives -** Initiatives are led by coordinators and can include non-members. The frequency and location of activities are to be decided upon by the coordinators. The initiatives progress will be presented annually and reported upon via the Secretariat.

- **Hosting the next GFCE meeting** - The next GFCE meeting is announced for 2nd quarter 2016.

  Point of action: Members are invited to express their interest to the Secretariat (at contact@thegfce.com) to host the next meeting by 1st February 2016.

  The African Union (AU) and the Organization of American States (OAS) have already offered their willingness to host the following meeting.

The GFCE Secretariat will be responsible for the administrative, logistical and analytical support and is available for all members. After the initial four years the members will evaluate the structure, operation, financing and location of the Secretariat.

The Secretariat consists of 5 persons, resides in The Hague and has the following tasks:

1. Be the main point of contact for all members;
2. Give support to initiatives;
3. Organize the annual high level GFCE meeting;
4. Contribute to matchmaking between members and members and partners.
5. Sharing relevant information among members and partners.

The Secretariat will provide the members with a ***catalogue of services*** to assist them with the initiatives. A first version of the catalogue will be shared in February 2016.

The website (www.theGFCE.com) will serve as information sharing point; displaying a summary of the initiatives and Q&A, the agenda for upcoming events and expert meetings and to communicate progress reports.

Members are periodically requested to send updates, including ongoing activities, on their initiatives (at contact@thegfce.com).

Breakout sessions on current initiatives

1. **Cybersecurity Awareness & a Global Campaign for Cybersecurity Awareness**

   Initiators: Canada, US, OAS, Senegal, the Netherlands

   Outline: The various awareness campaigns of the initiators work together in order to provide networks of expertise, pool resources and create a space for dialogue.

   Key message: governments are advised to build robust People Public Private Partnerships

   The OAS produces specific country assistant toolkits, to raise public awareness. These toolkits are focused on the governments and therefore work top-down. The Netherlands and Senegal organize two expert meetings in February 2016 and September 2016 and focus on the West African region.

2. **Cyber Security and Cybercrime Trends in Africa**

   Initiators: African Union, Symantec, United States of America

   Outline: By means of technical data analysis this awareness initiative aims to provide insight in the broader cyber security and cybercrime trends in Africa. Coming early 2016 the first phase of gathering information through questionnaires will be ready.

   What lessons learned could be passed along for increasing cyber security and fighting cybercrime in the African region?

   - African region, like other developing regions in the field of ICT, leapfrogged and skipped several steps in ICT Development (they have a strong mobile industry for example). What is needed is more attention to the user perspective or local perspective (local vendors and supporters).
   - Local partnership, building trust from bottom-up is key. For example, ISOC (present in Kenya and Nairobi) can be a resource, just like governments and private sector in receiving advice.

3. **Assessing and developing cyber capability**

   Initiators: United Kingdom, Republic of Korea, OAS, Norway, Global Cyber Security Capacity Centre

   Outline: The audience was presented an update on the initiative in general and the Oxford cyber capability model in particular. In this initiative, the Oxford model will be used to academically assess and rank the cyber capabilities of countries and organizations. This is done by assessing on 5 dimensions: a policy and strategy dimension, a cultural dimension, an educational dimension, a legal dimension and a technological dimension. Being in the pilot season, the model is still being developed itself. Pilots have been done through the OAS and are planned in Norway, the Republic of Korea and the Netherlands. In the presentation of the Republic of Korea the importance was stressed of defining roles and responsibilities, constructing a partnership plan and focusing on training and education.

4. **Cyber Security Initiative in OAS Member States**

Initiators: OAS, Mexico, Spain

Outline: OAS supports governments in drafting national cyber security strategies, organizes trainings, CSIRT exercises and crisis management exercises. In collaboration with various governments such as Mexico and Spain the OAS tries to increase the cybersecurity of the overall region. This occurs on a country-to-country basis but also aims to produce general pools of expertise. This session highlighted that the expansion of access which might lead to social and economic development, should be accompanied by a basis of cyber security. The OAS articulated their interest in expanding their activities to other regions.

5. **Responsible Disclosure Initiative**

Initiators: Netherlands, Hungary, Romania, Hewlett Packerd

Outline: This presentation highlighted the asset white hat hackers or ethical hackers might have for various organizations and governments. By bringing various security breaches or problems to the attention of the company or government etc. the overall safety of the net can be increased through a quick fix. To ensure ethical hacking is incorporated in a safe way public private partnership and good criminal codes are important. In the first quarter of 2016 Hewlett Packerd, Romania, Hungary and the Netherlands will organize a meeting in which best practices can be shared.

6. **CSIRT Maturity Initiative**

Initiators: Netherlands, OAS, Microsoft, ITU

Outline: In this session the Netherlands presented a CSIRTs toolkit which is geared at enabling the setting up of a CSIRT and will be used in the GFCE framework to assess the maturity of CSIRTs.

In addition Microsoft, ITU and OAS explained the importance of investing in CSIRT maturity, recognized the broad demand for CSIRT maturity practices and capacity and stressed the significance of a collaborating worldwide network of CSIRTs with bundled expertise to raise the general, global level.

Upcoming expert meetings: scheduled in January 2016 and the second quarter of 2016.

Pitches for potential GFCE initiatives

During the kick off meeting 3 pitches were presented on the following subjects:

A. Critical Information Infrastructure Protection(CIIP)

Who: Spain

Topic: The pitch proposed to combine the efforts on CIIP done in the Meridian conference framework, currently chaired by Spain, with the capacity building efforts of the GFCE, noting that there is a lack of such an initiative on a global scale.

This initiative has gained sufficient participants and is currently being proposed to GFCE member focal points as a formal GFCE initiative.

B. Implementing reliable Internet standards

Who: The Netherlands, Dutch Internet Standards Platform

Topic: The pitch aims for combining international efforts to implement modern internet standards (core internet standards) that strengthen overall cyber security.

Action point: Contact Mr. Gerben Klein Baltink directly to express your interest at gerben@internet.nl

C. CyberGreen

Who: Japan Computer Emergency Response Team (JPCERT/CC)

Topic: The CyberGreen initiative seeks to improve cyber health through mitigation and measurement, providing a platform for statistics and information sharing mechanisms. In doing so it seeks to empower the evolvement of metrics, capacity building efforts and a conference and advocacy program.

Action point: Contact Ms Yuri Ito directly to express your interest at yito@cybergreen.net

Contents

Day 1: Monday November 2th 2015

1. Opening GFCE Kick off meeting (13.00-13.20)

Uri Rosenthal, former Dutch Minister of Foreign Affairs and Special Envoy International Cyber Policy, opened the kick off meeting. He warmly welcomed all the guests and was pleased to see the evolvement the GFCE has been going through, in terms of initiatives, members and organization.
Subsequently, Wouter Jurgens, Head of Task Force International Cyber Policies MFA, gave a brief outline of the agenda and welcomed the presentation of the initiatives. Moreover, he hoped that these two days would be fruitful in terms of networking with other initiatives and spreading knowledge and expertise.

Goals of this meeting:

- To agree on the GFCE organisation and structure for 2015 and 2016
- To present an overview of the current GFCE initiatives and pitches for potential GFCE initiatives
- To network with other GFCE members and experts
- To obtain familiarity with the GFCE Secretariat and what it could do for you

2. Breakout session A: Cybersecurity Awareness & a Global Campaign for Cybersecurity Awareness (13.20 – 14.20)

By Mr Thomas A. Dukes – Deputy Coordinator for Cyber Issues – U.S. Department of State, Cindy Nelson MFA Canada, Joana Lehay US, OAS Kerry-Ann

In this presentation various country representatives explained how their respective countries realize awareness about cybersecurity. The campaigns were all directed towards the end-user of the internet and highlighted their responsibility. The key message of these campaigns: in order to enhance cyber security governments should find robust People Public Private Partnerships and other coalitions. This is to ensure that those who will get or already have access to the internet will know how to stay safe and secure.

The various awareness campaigns work together in order to provide networks of expertise, pool resources and create a space for dialogue. Despite the unique cultural environment of each country, by forming coalitions together this global problem can be effectively addressed. The OAS produces specific country assistant toolkits, to raise public awareness. These toolkits are focused on the governments and therefore work top-down. This to ensure that cyber security awareness is accepted on the political agenda.

3. Breakout session B: Cyber Security and Cybercrime Trends in Africa (13.20 – 14.20)

By: William Wright – Director Government Affairs & Cyber Security Partnerships – Symantec Corporation

Iinitiators: African Union, Symantec, United States of America.

Goals of this meeting was to provide an update on efforts of the initiative, discussing future efforts and gathering feedback from the audience. Cyber Security and Cybercrime Trends in Africa is an awareness initiative. It notes that “Digital isolation is quickly changing, Africa being at the threshold of an internet boom”. This provides both opportunities and risks. On one hand, Africa’s IT infrastructure will grow immensely. On the other hand cybercrime will grow accordingly. Therefore, there is a strong need for technical data analysis to provide insight in the broader cyber security and cybercrime trends in Africa, which this initiative aims to provide. In doing so, it uses the analytic capabilities and access to information of its initiators Symantec Corporation and the USA.
Coming early 2016 the first phase of gathering information through questionnaires will be ready. In order to gather input for the next phase of the initiative, two questions were posed to the audience. This resulted in a lively, detailed discussion with the audience and William Wright that proved fruitful for both parties.
Question one, regarding points of departure in securing Africa’s infrastructure and fighting cybercrime, resulted in a discussion on how Africa can “leapfrog” and avoid pitfalls that have occurred in Europe and the USA. The audience recommended an active discussion with policymakers, in order to keep the playing field small and provide clarity on definitions used.
In question two, regarding overcoming the difficulties of cooperation with multi-national organizations, the issue of trust was discussed. The audience suggested an approach based on local partnerships and building up trust from the ground level.

Why Africa?

- Very unreliable threat information in the continent
- Trying to be ahead of the curve since the internet boom for Africa is on the doorstep.
- 78% of internet use is directed to social media
- Simultaneously, there is an equal development of cybercrime
- Symantec threat intelligence has one of the most developed and sophisticated threat intelligence systems. With these great resources they can provide a good overview of the threat landscape, which will be strengthened by the survey they have sent out.
- Symantec is working on a global map of incoming and outgoing malware
- They have also set up a global government partnership

What lessons learned could be passed along to increasing cyber security and fighting cybercrime in the African region?

- African region, like other developing regions in the field of ICT, leapfrogged and skipped several steps in ICT Development (they have a strong mobile industry for example). What is needed is more attention to the user perspective or local perspective (local vendors and supporters).
- Local partnership, building trust from bottom-up is key.
- For example, ISOC (present in Kenya and Nairobi) can be a resource, just like governments and private sector in receiving advice.

4. Pitch new initiative: Critical Information Infrastructure Protection (14.35 – 14.55)

By Ricardo Mor Solá - Ambassador-At-Large for Cyber Security - Ministry of Foreign Affairs and Cooperation – Spain

The goal of the meeting is to find support for a new initiative building upon the Meridian Conference framework for Critical Information Infrastructure Protection

In the plenary session, Ricardo Mor Solá of Spain was given the floor for 20 minutes to pitch a new initiative on Critical Information Infrastructure Protection (CIIP). In the pitch it was proposed to combine the efforts on CIIP done in the Meridian conference framework, currently chaired by Spain, with the capacity building efforts of the GFCE, noting that there is a lack of such an initiative on a global scale.

The initiative aims to support policymakers in understanding the implications of CIIP, to raise awareness for the importance of CIIP as a vital component of cyber security and to make a broader audience benefit from the Meridian CIIP efforts.

Meridian and GFCE members that support the new initiative and are willing to co-sponsor with funding and expertise include Norway, Switzerland, Spain, and the Netherlands. Mr. Mor-Sola concluded his pitch with calling upon the GFCE members for support.

Aim of the initiative:

- Intended to support policy makers with the responsibility of the critical information infrastructure protection;
- Awareness raising of CIIP as a vital element of cyber security;
- leverage the expertise of the Meridian for the benefit of cyber security, especially in developing countries;
- To involve private partners as observers;

- Capacity building in the field of CIIP, as well as linking the expertise of the Meridian process on this domain to policy workers.

This is a good example of an initiative that was already set up but that can be improved or reach a greater audience through the GFCE.

5. Pitch new initiative: Implementing reliable Internet standards (14.55 – 15.15)

By Mr Gerben Klein Baltink- Chairman of the Dutch Internet Standards Platform

Conveying modern internet standards (core internet standards) that strengthen overall cyber security like ip6 are difficult measures for individuals to implement on their own. Therefore we are looking at organisations (NGOs such as internet society) that make it accessible for the general public and small and medium size businesses.

Difficult to find that one organisation that is responsible to implement TLS or other modern internet standards. Therefore it's a challenging task to get all the relevant players around the table to promote implementation of these standards.
Tooling is great, but the next step in limiting the risks is very important (for example in implementing TLS).

Offer people an insight in the standards that make up the internet.

6. Shooting for Longer-Termism in Cyber Security Capacity Building (15.15 – 15.45)

By Prof Michael Goldsmith (Senior Research Fellow - Dept of Computer Science - University of Oxford), Lara Pace (Knowledge Exchange Manager – Global Cyber Security Capacity Centre)

5 dimensions that look at multifaceted environments from policy area, cyber security, private sector, technical

Develop a global team for capacity building and develop a strategy to understand who is investing or implementing what and moreover to prevent that everybody is running behind the same ball. Strategy based on the thought to have a more global collective approach to capacity building. The mapping initiative truly is a global initiative with 200 experts, so it's an iterative approach, not an Oxford product to give an insight where and how capacity building is developing. The maturity model is an important element of the GFCE – the maturity model is an excellent first step to improve regional and global initiatives.

7. Breakout session C: Cyber Security Initiative in OAS Member States (16.00 – 17.00)

By Ms Kerry-Ann Barrett- Cyber Security Policy Specialist - Inter-American Committee against Terrorism - Secretariat for Multidimensional Security - Organization of American States

Ms Kerry-Ann explained that the OAS supports governments in drafting national cyber security strategies, organizes trainings, CSIRT exercises and crisis management exercises. In collaboration with various governments such as Mexico and Spain the OAS tries to increase the cybersecurity of the overall region. This occurs on a country-to-country basis but also aims to produce general pools of expertise. This session highlighted that the expansion of access which might lead to social and economic development, should be accompanied by a basis of cyber security. The OAS articulated their interest in expanding their activities to other regions.

8. Breakout session D: Assessing and developing cyber capability (16.00 – 17.00)

By Prof Michael Goldsmith (Senior Research Fellow - Dept of Computer Science - University of Oxford), Lara Pace (Knowledge Exchange Manager – Global Cyber Security Capacity Centre) replacing Tony Clemson (Head of Capacity Building, Prosperity, Cyber Crime – Cyber Policy Department – Foreign and Common Wealth Office – United Kingdom), Hongsoon Jung (Representative of the Republic of Korea)

Initiators: Norway, Organization of American States, United Kingdom

Goal of the Meeting provide the audience an update on the initiative in general and the Oxford cyber capability model in particular. The presentation of the initiative Assessing and developing cyber capability would have been given by Tony Clemson, representative of the United Kingdom, but due to his plane being delayed by fog, Lara Pace and Professor Michael Goldsmith of the University of Oxford replaced him. The presentation was mostly an elaboration of the Oxford University model to assess cyber capability introduced in their plenary presentation.

In this initiative, the Oxford model will be used to academically assess and rank the cyber capabilities of countries and organizations. This is done by assessing on 5 dimensions: a policy and strategy dimension, a cultural dimension, an educational dimension, a legal dimension and a technological dimension. Within these dimensions, the descriptor of the level of maturity is based on 48 indicators. Eventually this assessment can be used to advise countries or organizations on developing their cyber capability.

Being in the pilot season, the model is still being developed itself. Pilots have been done through the Organization of American States and are planned in Norway, the Republic of Korea and the Netherlands. One

of these pilot cases – the Republic of Korea – was given the floor to present on the particular capacity building experiences in the respective country. In the presentation, Mr. Hongsoon Jung of the Republic of Korea stressed the importance of defining roles and responsibilities, constructing a partnership plan and focusing on training and education.

Afterwards, the floor was opened for questions by the audience, which resulted in questions on including the multiple stakeholder approach in the model, the concept of harm and the importance of defining roles in applying the model.

Day 2: Tuesday November 3th 2015

9. GFCE Organization and Structure (9.15 – 10.25)

Wouter Jurgens Head Task Force International Cyber Policies – Ministry of Foreign Affairs – the Netherlands gave a presentation on the proposed Terms of Reference:

a. The Netherlands will be chair for the next coming four years. As indicated in the ToR, the introduction of a co-chair would be welcomed.
b. New members will be admitted during GFCE meetings, which will be held at least once a year.
c. The initiatives are led by coordinators and can include non-members. The frequency and location of activities are to be decided upon by the coordinators. The initiatives' progress will be presented at GFCE meetings and on the website www.theGFCE.com.
d. The Secretariat will be responsible for the administrative, logistical and analytical support and is available for all members. They will provide a catalogue of services to assist members with their initiatives. After the initial four years the members will evaluate the structure, operation, financing and location of the Secretariat
e. The Netherlands proposed the installment of an Advisory Board. The GFCE Advisory Board constitutes of representatives of civil society, technical community and think tanks and provides non-binding but informed guidance to the GFCE members.
f. Proposing the installment of a co-chair, this is renewable every four years. Aim is to balance the chairmanship geographically. Members can express their interest before the 1st of February.

In general there was a lot of agreement about the ToR, and members are invited to send their written comments the coming month.

Reactions from members:

- **The African Union and the OAS** indicated their willingness to host the following meeting.
- During the discussion questions rose whether there was a maximum of projects and members. Considering the NL no threshold is necessary but important to balance both efficiency and effectiveness with participation. The GFCE should remain an open platform and therefore membership and initiatives should remain open for others. Especially in some thematic and regional areas there is room for more initiatives.
- **Spain** wondered whether the secretariat should approve if the objectives of new initiatives are in line with the overall GFCE mandate, which according to the NL is not the responsibility of the Secretariat but of the members. New initiatives might be adopted either via an annual meeting or initially via a written procedure. It is important that new initiatives are endorsed and presented within the GFCE.

- **CISCO** wondered whether accepting many others as members would contribute to losing the focus of the GFCE. The NL emphasized hereon that numbers are to a certain extent limited, as the focus should be on who can contribute.
- **OAS** questioned the usefulness of a work plan; NL replied that the work plan would ensure that all members of the GFCE are aware of the various initiatives and can track the progress that is reached. Moreover, the work plan would contribute to the outreach the GFCE aims for, to share knowledge with others.
- **Canada** wondered if the process of the GFCE is still linked to the London process. This is the case, but some flexibility is required as the next conference date has not yet been communicated.
- **Germany** was questioning if it would be useful if there would be a difference between internal and external communication about the initiatives. Although the GFCE is a member based organization, the need for capacity building and sharing expertise should be central. Therefore, the results of the initiatives should be shared widely through the website and accessible to a broader public.
- **US:** it would be useful if clarity would be created about what initiatives are executed where and what expertise/interest which country has. The portal link of the Oxford Cyber-security world wide- at a glance, would solve this problem partly. Moreover, the Secretariat will provide a questionnaire as to identify what the interest and priorities of the various members are.
- **Microsoft/CISCO**: the GFCE is unique in the approach it takes, which is completely open source. It should aim to remain that open character. Moreover, it would be helpful if members can contribute resources without being a coordinator. NL agrees with both of these remarks.

10. Secretariat (10.25 – 10.45)

By David van Duren (Head of the GFCE Secretariat) and Carolin Weisser (Portal manager at the Global Cyber Security Capacity Centre, University of Oxford).

The Secretariat consists of 5 persons and is hosted at the Hague Security Delta campus. The mission of the GFCE Secretariat is simply ‘making the GFCE a success’. The Secretariat has the following tasks:

1. Be the main point of contact for all members;
2. Give support to initiatives;
3. Organize the annual high level GFCE meeting;
4. Contribute to matchmaking between members and members and partners.
5. Sharing relevant information among members and partners.

The website will serve as information sharing point; displaying a summary of the initiatives and Q&A the agenda for upcoming events and expert meetings and to communicate progress reports. All members are welcome to send updates on their initiatives.

Ms Carolin Weisser gave a presentation on the portal of Global Cyber Security Capacity Centre. This portal, developed in partnership with the GFCE, shows international, regional, and national projects, programmes and activities that aim to build cyber capacity worldwide.

It helps to enhance global cyber capacity by allowing actors to share their experience, access information on solutions and strategies, and open up space for collaboration.

11. Breakout session E: Responsible Disclosure Initiative (11.00 – 12.00)

By Mr. Hans de Vries – Head National Cyber Security Centre - Ministry of Security and Justice – the Netherlands

Responsible disclosure is the detection of vulnerabilities by ethical hackers, enabling organizations to tackle and repair the risks these vulnerabilities pose. This conclusion was explicitly emphasized during the Responsible Disclosure breakout session. In drafting up this conclusion, the distinction between criminal, 'black hat' hacking and ethical 'white hat' hacking was discussed. Both hackers focus on detecting vulnerabilities, the latter however without criminal intentions. The Netherlands introduced this distinction and the subject of responsible disclosure with a video of ethical hackers stating their intentions.

Responsible disclosure is an accepted way of handling vulnerabilities in the Netherlands. Central to this acceptance is the belief that hackers should be prosecuted based on intention: hackers with the right intentions should not be punished. Although successful in the Netherlands, this belief is not globally shared. The initiative posed the question if this should change, triggering positive reactions. For example in Hungary, one of the participants in the initiative, ethical hacking is under certain conditions already legal. Another positive reaction came from Latvia, emphasizing the need of a European legal framework for responsible disclosure, which could possibly be a combined message communicated through the Dutch 2016 Presidency of the Council of the European Union. 'At least as important as the option to responsibly disclose detected vulnerabilities are the actual repairs' is the second Latvian argument, 'for if companies and institutions do not adequately react to detected vulnerabilities, ethical hacking loses its function.'

Cisco Systems specifically mentions 'The Internet of Things, but I prefer to call it the Internet of Threats'. In handling the Internet of Threats, the strengthening of networks is a crucial solution and 'if there are no solutions available, it could be possible to create a work-around within a network'. Within this example lies the strong need for cooperation between the public and private sector.

The Netherlands concluded and announced that two expert meeting will be organized in 2016. In the first meeting experiences will be shared on responsible disclosure and developing ethical hacking capability as a part of a broader process raising cyber resilience. In the second meeting experts will be encouraged to start developing a best practices document or framework document for responsible disclosure and developing

ethical hacking capability as a part of a broader process raising cyber resilience. GFCE members expressed their interest to attend the expert meetings.

12. Breakout session F: CSIRT Maturity Initiative (11.00 – 12.00)

By Aart Jochem (Head Monitoring and Response – National Cyber Security Centre - Ministry of Security and Justice – the Netherlands), Jochem de Groot (Government Lead Benelux, Microsoft), Don Stikvoort (M7), Martijn de Hamer (Ministry of Security and Justice – the Netherlands), Luc Dandurand (International Telecommunication Union) and Kerry-Ann Barrett (Cyber Security Policy Specialist - Inter-American Committee against Terrorism - Secretariat for Multidimensional Security - Organization of American States)

Initiators: Netherlands, ITU, OAS, Microsoft

Breakout session F included four presentations on the CSIRT Maturity Initiative, moderated by Aart Jochem, Head of Monitoring and Response of the National Cyber Security Centre the Netherlands.

The first presentation by Don Stikvoort and Martijn de Hamer introduced the CSIRTs toolkit developed by the Netherlands. The toolkit is geared at enabling the setting up of a CSIRT and will be used in the GFCE framework to assess the maturity of CSIRTs. An in depth explanation of the toolkit's mechanisms followed, including an explanation of the 5-tier model used to assess CSIRT maturity.

The second presentation by Jochem de Groot, representing Microsoft, explained Microsoft's views and principles on the importance of investing in CSIRT maturity. De Groot stressed the significance of a collaborating worldwide network of CSIRTs with bundled expertise to raise the general, global level.

The International Telecommunication Union (ITU), represented by Luc Dandurand, presented the broad activities undertaken by the ITU to raise CSIRT maturity. In their extensive existing efforts, the ITU observed the sheer amount of demand on CSIRT maturity practices and realized that only through international collaboration this need can be met. Therefore, the ITU expressed their content with the opportunity the GFCE offers to combine their efforts internationally.

In the following presentation, the Organization of American States (OAS), accordingly observed a lack of CSIRT capacity in the OAS region and expressed their willingness to further contribute to the CSIRT Maturity Initiative to tackle this problem.

The audience agreed that the CSIRT Maturity Initiative is a perfect example of how existing efforts can be combined and effectively be applied on a global scale for the benefit of all, serving the overarching goal of increasing the outreach cyber capability and improving cyber resilience. The initiative additionally presented its planned steps forward, including upcoming expert meetings in January 2016 and the second quarter of 2016.

Quick scan:
42 organizations filled out the quick scan since April. The initial level of the results of these tests indicate that the maturity level is fairly low, which shows that there is need for this initiative.
Expert meetings coming up in 2016: Prague 27 January 2016 (best practices) and June 2016, data and location TBC.

ITU
65 assessments that have been done by ITU (3-5 day workshops)
Holistic approach that takes into account the national strategy as well as the involved organs and the national security. Their assessment is much more than only CERT functioning, but applies to wider cyber security.

Increasing maturity is key to building confidence and security in the use of ICTs. Create an overview of all the initiatives in the Oxford portal.

OAS
Basic capacity and incident response teams
Capacity is required both in human capacity as in technical expertise. CERTs cannot jump to the level of a mature CERT, but you need to look at being most effective for your constituency, which demands trust and a tailored approach. A Portal (private network) will be developed in which CERTS can share tools with each other, upload data or any other source of data. The future of this portal is how law enforcement agencies can benefit from this portal.

All parties encourage a hands-on approach to incident response and capacity building in this area.

13. iHUB (13.15 – 14.00)

Presentation by Mr. Kirui Kennedy on the iHUB organization based in Nairobi, Kenia.

iHUB is an inspiring example in Africa where people and their expertise are being brought together in order to learn, share and innovate. iHUB connects people and startups by providing unique and innovative tech services.
The stimulating environment also acts as a sandbox for innovation, appropriate infrastructure, focused training, startup incubation as well as holding high impact events.

14. Pitch new initiative: CyberGreen (14.00 – 14.30)

By Yurie Ito (Director of Global Coordination Division for the Japan Computer Emergency Response Team (JPCERT/CC)

With the aim of finding support and funding among GFCE members, the existing CyberGreen initiative was pitched to GFCE members.

The CyberGreen initiative aims to make cyberspace more sustainable. It observes that policy in cyberspace mostly related to security and therefore response driven. It argues that we should develop long-term solutions, based on prevention and improvement rather than response. Applying analogies from other fields to cyberspace, Yurie Ito argues that it should be greener, cleaner and safer, build on a green field rather than a swamp.

Translated to actions, the CyberGreen initiative seeks to improve cyber health through mitigation and measurement, providing a platform for statistics and information sharing mechanisms. In doing so it seeks to empower the evolvement of metrics, capacity building efforts and a conference and advocacy program.

CyberGreen concerns a non-profit and global initiative that aims to improve the cyber health.
Securing up your own environment is not sufficient anymore; we depend on the security and clean systems of our colleagues, peers and partners. Moving beyond an individual-based cyber security of building walls (response) to a regional or even global way for prevention and improvement.

We are responsible for taking care of our own clean pc: once these devices are infected, not only our credentials are at risk, but our devices can serve as proxy attack. CyberGreen not only cleans up, it is also doing metrics: how many infected machines in our space? Are we improving or are you a polluter?

We need to improve the quality insurance of our technical ecosystems: we need to regain the trust of the users and companies. This initiative aims to reach out to the root cause of the malware and infections (instead of the traditional measures that aim at the consequences or symptoms).

15. Closing and next steps

By Wouter Jurgens (Head Task Force International Cyber Policies – Ministry of Foreign Affairs – the Netherlands), Patricia Zorko (Deputy National Coordinator for Security and Counterterrorism & Director of Cyber Security – Ministry of Security and Justice – the Netherlands) & Mr Hans de Vries (Head National Cyber Security Centre - Ministry of Security and Justice – the Netherlands)

The conference was concluded in a plenary session with 3 speakers of the hosting country. Wouter Jurgens, Head Task Force International Cyber Policies of the Ministry of Foreign Affairs, provided the audience a recapitulation of the conference. Expressing his content with the contribution of the GFCE members and partners present, Wouter Jurgens summarized the conference and next steps to be taken by the GFCE. This included the Terms of Reference, Initiatives, Co-chairmanship, Advisory Board and next meeting.

Giving her first speech as Deputy National Coordinator for Security and Counterterrorism & Director of Cyber Security of the Ministry of Security and Justice, Patricia Zorko stressed the importance of cyber security in the broader sense. She warns that “if we lack in our combined efforts, a free, open and secure internet will be

reduced to words spoken on conferences". She concluded with expressing her gratitude to the efforts being made by the members of the GFCE.
In the final remarks, Hans de Vries (Head National Cyber Security Centre, Ministry of Security and Justice) expressed his appreciation of the GFCE members, initiatives and the organization of the GFCE International Kickoff Meeting. Concluding that "awareness is easy to say but difficult to realize" he stressed the importance of international collaboration.

Points of Action List

Action/decision	Background	Timeline
Adoption of GFCE Terms of Reference (ToR)	The draft ToR (see attached) outlines the structure of the GFCE. This document is an operational follow up on the 'GFCE Framework Document' and the 'The Hague Declaration on the GFCE' which were adopted during the GCCS2015.	Share your comments by 30th Nov 2015 Final ToR circulated to members by 15th Dec 2015
Proposal new initiative: Critical Information Infrastructure Protection	See description of initiative in attachment. This initiative will be jointly developed by Norway, Switzerland, Spain and the Netherlands	Comments by 30th November 2015 (silent procedure)
Sharing information on ongoing GFCE initiatives	In order to facilitate your initiative and to share information via the website with other members we are looking for the following information: Summary of initiative (check on site if current summary is correct), planning/agenda of activities (initiative meetings), related documents.	Send us your updates by 30th November. In the coming weeks the secretariat will also pro-actively contact initiators of initiatives individually.
Expression of interest to new possible initiatives	Two other potential new initiatives are still looking for more participants. Contact the initiators directly to express your interest: Ms Yuri Ito for 'Cybergreen' (see also attachment) (yito@cybergreen.net) and Mr. Gerben Klein Baltink for 'implementing reliable Internet standards' (gerben@internet.nl).	Express your interest by 31st December.
Expression of interest GFCE Co-Chair	The ToR proposes two Co-Chairs to coordinate the work of the GFCE and prepare international meetings (in collaboration with GFCE secretariat). The Netherlands has been proposed as one of the co-chairs, a second co-chair position is vacant.	Express your interest to become co-chair by 1st Feb 2016
Host for next High Level GFCE Meeting	Suggested time frame next meeting; 2nd quarter 2016. To ensure geographical representation preferably in Asia, Africa or the America's.	Share your interest to host the next meeting by 1st Feb 2016
Establishment of Advisory Board	In order to ensure inclusion of cyber related NGOs, the tech community and academics in the GFCE an Advisory Board will be established. A proposal for this Advisory Board will be drafted by the GFCE chair and circulated to GFCE focal points for decision.	Draft proposal will be circulated by 1st Feb 2016 Share your comments and propose partners by 15th Feb 2016