GFCE
Global Forum on Cyber Expertise

31 MAY > 01 JUNE > BRUSSELS

GFCE Annual Meeting 2017

Report by the GFCE Secretariat

Day 0 – May 30

On May 30, the GFCE Secretariat organized two pre-Annual Meeting workshops. The aim of these workshops was to focus with a targeted group on two themes that are vital in the context of the GFCE.

The morning workshop was on the concept of Global Good Practices (GGP). In a session moderated by DiploFoundation, participants discussed what a global good practice is, and how GFCE can best distil the GGPs of its global initiatives. This workshop aimed to encourage the representatives of GFCE initiatives and other participants to look at their work using a capacity development lens, applying some of the key concepts and approaches from this field to discuss GGPs. In smaller groups, participants explored tools, challenges and suggestions to measuring the impact of a practice or an initiative.

In the afternoon, TNO, the Netherlands Organisation for Applied Scientific Research, moderated the workshop 'Sharing Experiences on Cyber Capacity Building (CCB)'. With representatives from donors and receivers present, the workshop touched several issues regarding effective and efficient cyber capacity building. Gaps in CCB were identified; dimensions of a country's cyber security maturity were discussed; project leads of CCB projects shared their experiences on (the challenges and successes of) local cyber capacity building; and all participants elaborated on what they think is needed for effective CCB in their region.

*Please see **Annex 1** (page 20) and **Annex 2** (page 23) for an elaborate overview of the workshops on May 30.*

Day 1 – May 31

09.00 – 09.50 Official opening remarks

Official word of welcome by **Ms. Carmen Gonsalves** (GFCE co-chair, representative from the Netherlands)

- The GFCE has grown to 60 members; new members include Singapore, OSCE, AT&T, Commonwealth Telecommunications Organisation, INTERPOL, World Bank, International Association of Prosecutors, Surinam.
- GFCE has ambitious goals: to be the coordinating body for cyber capacity building on a global scale, both as a knowledge sharing platform as well as a forum for cooperation.

Opening speech by **Mr. Pawel Herczynski** (EEAS)

- Cyberspace is borderless; therefore international cooperation is key in cybersecurity.
- The GFCE is important as a means of coordination between different stakeholders and to avoid duplication of existing efforts in the field.

Keynote speech by **Ms. Aruna Sundararajan** (GFCE co-chair, representative from India)

- The GFCE needs to be a pragmatic, action-oriented forum.
- With 60 members covering two-thirds of the global population, we have a common platform for common challenges.
- India is dealing with challenges in CCB; wants to achieve more cyber inclusiveness and a cashless society through the *Digital India Programme*.
- India has a strong focus on E-governance regarding cyber capacity building.
- India sees the future of the internet as part of the Global Commons; free, open and secure.

09.50 – 10.30 Panel Discussion: The strategic context of cyber capacity building

Panel discussion by **Mr. Uri Rosenthal** (Global Commission on the Stability of Cyber Space), **Ms. Kaja Ciglic** (Microsoft) and **Ms. Nayia Barmpaliou** (European Commission).

The panel broadly recognized that cyberspace is climbing up on the political agenda. At the same time, this growing awareness is in many cases fostered by incidents, resulting in ad hoc forms of cooperation. In the near future, these ad hoc partnerships will have to develop into a more organic and continuous flow of cooperation. Such development requires a mental frame of working together and sharing information – not just between governments, but also including the civil society through the multistakeholders approach.

Meanwhile, there is a growing need to prioritize cyber capacity building (CCB) on a strategic and operational level. Breaking down the silos and creating a framework for public-private cooperation is essential, while consolidating what is already there. In this regard the GFCE needs to further evolve into a coordinating platform on how to deal with things from a methodological perspective. Whilst the need for a coordinating mechanism is evident, one needs to take into account that people become more and more connected – also in different ways (AI, IoT). Therefore, it is crucial to think about what that means for cybersecurity professionals.

With the growing connectivity in every region of the world one can identify the emergence of different cyber 'cultures', where people connect differently and with different products. Efforts from the 'western world' need to take this into account, addressing this as a *two-way exchange*.

11.00 – 12.15 Working session I: Global Agenda priority setting

The primary objective of this session was to prioritize topics of interest to be included in the Global Agenda on Cyber Capacity Building (GACCB). The resulting list of key topics of interests from participants will form the foundation for the GACCB.

Based on analysis of a wide collection of national and international cyber strategy documents, TNO had prepared a list of potential topics of interest. **Ms. Tjarda Krabbendam** (TNO) introduced TNO's working method and the desk research done on the GACCB so far. The list of potential topics of interest contained topics on a strategic, tactical and operational level, and provided a comprehensive overview of global topics of interest as set forth by governments and international organizations. This gross list was shared with participants as input to the roundtable sessions. Further elaboration was provided by the Oxford Global Cyber Security Capacity Centre (GCSCC), that presented their analysis of over 150 initiatives that are published on their cybersecurity capacity portal.

After the plenary introductions, the approximately 150 participants started their roundtable discussions. These consisted of three connected rounds: a prioritization session (round 1), an elaboration session (round 2) and a recapitulation, or recap session (round 3). In round 1,

participants were requested to prioritize among a long list of potential GACCB topics. In round 2, participants were asked to further outline challenges and ambitions on the selected topics.

13.30 – 14.30 Plenary: Recap Global Agenda

In round 3, the moderators were kindly requested to give a plenary recap about their roundtable findings. Beside sharing how and which topics their tables prioritized, the moderators shared some more general remarks and suggestions on the Global Agenda:

- *… that defining a baseline national approach should include a general strategy document, plan on CIIP and emergency response. Such a baseline should be a prerequisite for efficient international cooperation.*
- *… education and training was mentioned several times as a key priority.*
- *… writing down measurable targets and timeframes was a difficult task, though needed.*
- *… it is important to link and connect topics with each other as it was found that there is some overlap in themes and domains, but also in a certain sequence one should adopt in terms of importance and relevancy. Some topics also require subgroups of topics or a differentiation between specific and generic topics. Another approach suggested is to make packages with the most important topics, e.g. strategies, CIIP, CERT.*
- *… the strategic level is very important to focus on.*
- *… political will is crucial, but can be difficult to obtain.*
- *… cybersecurity is an enabler, not an end state.*
- *… apart from needing to know what is on a GACCB, it is also to address why.*
- *… that is important to quantify goals set, i.e. we need an GACCB that is SMART.*
- *… see data protection a human rights issue.*
- *… National Cyber Security Strategies are often amended or explained within a Digital or ICT strategy. We should not focus too much on the wordings of 'a NCSS'.*
- *… all timeframes need to be cyclical in order to revise every single topic that is mentioned and performed.*
- *… that is was difficult to separate national and international attention for topics.*

14.45 – 15.45 Breakout session: New (potential GFCE) initiatives (parallel sessions)

Smart Nation Vision and the Internet of Things

Mr. Hoo Ming Ng, Singapore

The vision is for Singapore to be a smart nation. A nation where people live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all. Launched by Prime Minister Lee in 2014, the key goals of the vision were to empower citizens and businesses and improve urban living through: (i) Increased access to data (ii) Increased contribution of innovative ideas and solutions (iii) Better whole-of-government Smart Nation coordination.

The Internet of Things (IoT) is an essential element for a Smart Nation. However, IoT and smart systems are increasingly at risk with the growing number of attacks. Threats are no longer

geographically bound; it is essential to have a secure and resilient cyberspace. Cybersecurity is now a key enabler in ensuring that Smart Nation aspirations are realized.

At this point there is a lack of understanding of security requirements by countries. Cybersecurity is a global and transboundary issue. As such, it is important to drive this effort with international partners. Singapore is keen to work with the GFCE to lead international efforts to study cybersecurity for IoT, come up with measures and best practices i.e. through a landscape study, technical references, IoT cybersecurity standards.

National Cybersecurity Strategies

Mr. Marco Obiso, ITU; **Ms. Kaja Ciglic,** Microsoft; **Mr. Fargani Tambeayuk,** CTO

In the presentation it is stated that current National Cybersecurity Strategy (NCSs) Efforts should be coordinated. The importance of having a NCSs is stressed. By developing and implementing its National Cybersecurity Strategy, a nation can improve the security of its digital infrastructure and by doing so contribute to its broader socio-economic aspirations.

Ideas regarding the outcome of this potential initiative are:

- An annual workshop to exchange best practices, as well as to assess the need to update existing materials and/or complement them with additional resources.
- Establishment of an access-controlled portal to share documents and coordinate activities by the members of the initiative.
- Creation of an open portal to showcase the initiative and highlight how individual countries can get support.
- Creation of a database of accredited individuals/groups that could deliver assistance.
- Research and development of metrics to measure success of NCSs.

GLACY+ (Global Action on Cybercrime Extended)

Mr. Mateo Lucchetti, Council of Europe

The GLACY+ project is a co-initiative of the EU and CoE and acts as a resource to support more than 130 States that implement the common standards of the Budapest Convention on Cybercrime, States which have laws largely in line with the Budapest convention or States who are drawing on the Budapest Convention for legislation.
GLACY+ is, together with other capacity building programs, being implemented by the Cybercrime Programme Office of the Council of Europe in Bucharest (C-PROC) who has the mission 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.

Specific focus of GLACY+ is on:

- Promoting consistent cybercrime policies and strategies as stand-alone and as part of broader cybersecurity;
- Strengthening the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions;
- Enabling criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation.

Key factors for capacity building in GLACY+ are:

- Clear definition of the scope,
- Local ownership and engagement of decision-makers,
- Regional outreach,
- M&E methodology and Embedded Metrics/Indicators
- Sustainability and Coordination with regional/ international organizations.

NoMoreRansom

Mrs. María J. Sánchez, EUROPOL

The No More Ransom portal is a non-commercial initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre and two cyber security companies – Kaspersky Lab and Intel Security – with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals. Furthermore the initiative encourages reporting of ransomware, strives to disrupt the criminal business model and aims to arrest and prosecute suspects.

No More Ransom is a public-private initiative launched on 25 July 2016 which created a common portal (www.nomoreransom.org) which contains, among others:

- Available decryption tools for some of the existing ransomware families (offered by the project partners to the victims, free of charge);
- Tips and advice to prevent users from becoming a victim (educational and awareness material);
- Direct links to the national police agencies of the EU Member States to encourage the citizens to report the cases (one of the common problems law enforcement faces with this phenomenon is the lack of information to investigate further).

Capacity Development in e-Diplomacy

Mr. Iddo Moed, Israel**; Ms. Qendresa Hoxha,** Switzerland; **Ms. Tereza Horejsova** and **Mr. Vladimir Radunoviç,** DiploFoundation

Governmental activities are increasingly supported by Internet tools; this is no different with diplomacy. The capacities to deal with these changes are lacking in most institutions and stakeholders.

Aim of the new GFCE initiative is to:

- Raise awareness about the impacts of the digital transformation on diplomacy.
- Develop capacities of public institutions, diplomats, other stakeholders in smartly embracing e-tools in diplomatic practice + understanding of cyber issues on the diplomatic agenda.
- To enhance co-operation among various ministries and departments.
- Increase GFCE portfolio and visibility in the field of e-government.

The activities of the initiative will be based on 'awareness raising', e.g. e-diplomacy days and focused discussions during major cyber events, as well as on 'capacity development', e.g. customized short training sessions for diplomats and research, mapping and case studies.

Promoting implementation of Cyber Stability Measures

Mr. Velimir Radicevic, Organization for Security and Co-operation in Europe

Tools and frameworks for cyber stability already exist on the international and regional levels, which means that connecting, implementing and promoting them becomes imperative. On an international level, UN GGE reports provide guidance on norms of responsible state behavior in cyberspace, confidence-building, application of international law in cyberspace and promotion of co-operation. On REGIONAL levels we have organizations (e.g. OSCE, ARF, OAS, AU etc.) which are acting to operationalize this global guidance.

Objective: Increase awareness on, and promote cyber stability through the acceptance and application of practical measures and pertinent norms.

The initiative will:

- Link current discussions on cyber stability in regional and global fora.
- Explore the interlinkages between norms, agreed-on CBMs and awareness raising/capacity building.
- Accelerate the implementation of existing CBMs and socialization of norms.

Gender and Cybersecurity

Ms. Alison August Treppel, Organization of American States

The Gender and Cybersecurity initiative is initiated by Spain and currently co-sponsored by the General Secretariat of the Organization of American States (OAS). The goal of this initiative is to create a more inclusive digital world, along two parallel tracks:

1. Addressing the gender gap in the cybersecurity industry. It aims to both look into reasons behind the minor representation of women in the cybersecurity sector, as well as propose solutions to diminishing this gap.
2. Promoting policies to successfully counter online abuse and gender-based violence.

Activities and expected outcomes:

- Discussing good practices that 1) promote more inclusive career opportunities in cybersecurity and 2) raise the awareness among stakeholders about the difference in impact that cyber threats and cybercrime have on men and women.
- These discussions will take place during forums panel discussions and workshops. Attention is drawn to an expert meeting that was to take place in the very near future, June 5 and 6 in Leon, Spain.

E-Government

Mr. Ricardo Mor Solá, Spain

E-Government is a co-initiative between Spain and OAS. The results of a research by OAS, the Inter-American Development Bank (IDB) and the Global Cyber Security Capacity Centre (GCSCC), which indicated the maturity of cybersecurity in Latin American and Caribbean countries, have spiraled the E-Government initiative.

The research found in 87.5% of included Latin American and Caribbean countries, trust in e-government is low. Additionally, over 96% of the researched countries scored low on the cybersecurity mindset that is present in their governments.

To improve these scores, Spain and OAS aim to work together to share best practices on e-government from Spain, a country ranking #17 on the 2016 UN E-Government Survey, with Latin American and Caribbean countries.

16.15 – 17.15 Plenary: Update Global Initiatives

Moderated by **Pablo Castro** (Chile)

Critical Information Infrastructure Protection (CIIP)

Mr. Peter Burnett, Meridian & **Ms. Nynke Stegink**, the Netherlands

The Meridian community / conference brings together people from all time zones to the meridian spot. The conference takes place every year in a different location. It's mainly build on trust. The Meridian CIIP– GFCE initiative has worked on several elements:

- Organized expert meeting/ Buddying Program. Esp. developed countries together with developing ones.
- CIIP Good Practice Guide v1> tool for capacity building programs in other countries.
- CIIP is the most important bit of cybersecurity – if you don't do it everything fails.
- Primer Day (CIIP Training/Awareness Package)
- Memorandum to be produced.

Global Campaign to Raise Cybersecurity Awareness

Ms. Joanna LaHaie, US

The initiative is about: creating awareness of cybersecurity best practices; increase understanding of cyber threats and empower all citizens to be safe and secure online.

The initiative has 4 basic best practices:

1: finding means to foster cooperation and alignment of programs
2. Promoting of cyber safety resources
3: Events to raise awareness.
4: Cyber security awareness month (October).

Awareness campaigns are a joint effort of a cyber awareness coalition: global, national, local + NGOs, civil society, private industry and academia.

Added value of the initiative is:

- policy focus for governments
- Resources which can be used in different contexts
- Opportunity of outreach

CSIRT Maturity Initiative

Ms. Petra Nijenhuis-Timmers, the Netherlands & **Mr. Damir Rajnovic**, FIRST

This initiative is assisting emerging and existing CSIRTS to increase their maturity level. Several expert meetings are held in Seoul and Geneva. As a result, a concept good practices

memorandum has been developed. The initiative also includes a capacity building program which implements good practices on national CSIRTS by assisting parties to increase their maturity. Key objectives involve:

- Organizational changes, higher in the ministerial structure, closer to policy makers etc.
- Human changes (increased staffing + budget for training).
- Communication: clear roles, activities and lines in crisis situation.

Assessing and developing cybersecurity capability

Mr. Paul Cornish, GCSCC

Cybersecurity is not just threat management but also about the exploitation of opportunity. In that regard Oxford has assisted 17 countries in capacity review and is discussing the same approach with other countries. Oxford is involved with over 50 countries, roughly 25 percent of UN members. Examples are activities on e.g. CSIRTs, cyber strategies in Kosovo, Colombia, Jamaica, UK, Dominican Republic and Uganda. Not reinventing the wheel, collaboration is paramount. Furthermore capacity cannot be a sporadic series of national efforts: an international approach is key.

All the activities are supported by the Oxford Portal on CCB: Global repository with information on activities, progress, and on best practices.

Internet Infrastructure Initiative

Mr. Thomas de Haan, the Netherlands

Goal of this initiative is a healthy internet ecosystem: up to date, open interoperable, secure, future proof. Phase 1 of the project was adapting latest standards for email, web surfing, address space. This prevents eavesdropping, phishing and botnet abuse and aims to diminish the impact of cybercrime and cyber-attacks.

In the end, this will lead to more confidence and trust which is obviously a prerequisite for innovation and online economy. Progress of the project thus far: partners have been identified, needs have been assessed, now project planning

Products for the community are best practices documentation, a reference repository, and a testing tool available in 5 languages.

Coordinating Vulnerability Disclosure (CVD)

Ms. Petra Nijenhuis-Timmers, the Netherlands & **Ms. Mihaela Popescu**, Romania

The purpose of this initiative is to enable organizations in the public and private sector to make their own policies on ethical hacking. Cooperation with ethical hackers plays a central role. Within this initiative, two GFCE expert meetings were organized, in Budapest and Bucharest.

Deliverables and products of this initiative are:

- Promoting of CVD in EU High Level Meeting and OSCE;
- Memorandum on good practices including CVD policy and procedure models;
- Legal research;
- Further promotion of CVD at regional and international level.

17.15 – 17.30 Plenary: Wrap-up

During the wrap-up by the Dutch co-chair the 3rd edition of the Global Magazine on Cyber Expertise and the GFCE Cyber Monitor were presented.

Day 2 – June 1

09.00 – 09.15 Opening

Official word of welcome by **Ms. Aruna Sundararajan** (GFCE co-chair, representative from India). The program of day two of the GFCE Annual meeting was presented.

09.15 – 09.30 Advisory Board

The Co-chairs of the Advisory Board, **Ms. Lea Kaspar** and **Mr. Moctar Yedaly** give a presentation on behalf of the AB. The mission of the AB is to provide 'nonbinding but formal guidance to the GFCE Members on cyber capacity building'. This includes advice on GFCE initiatives. So fare the AB has provided input into the GFCE roadmap documents. Outreach to members and partners in order to further the GFCE goals and initiatives. AB members are committed to supporting members' capacity building actions.

The AB welcomes comments, questions and ideas from members and partners of the GFCE.

9.30 – 11.30 Working session II: Global Good Practices

Following up on the pre-day workshop discussion about the initiatives and partners involved, the plenary session further looked at what GGPs could be. The session consisted of three parts: an introductory 'setting the scene' presentation about the GGPs and the capacity development concept and practical links to GFCE work, the roundtable discussion in which aims, targets and achievements of each of the global initiatives was discussed in diverse small groups, and a recap with a debriefing by each group. Over 100 GFCE members and partners actively participated in the session and shared their views.

In the introductory part, **Mr. David van Duren** (Head of the GFCE Secretariat) reiterated the endorsed GFCE Roadmap plan to produce a set of GGPs in capacity building as one of the main deliverables towards the Global Conference on Cyber Space (GCCS2017). DiploFoundation's **Mr. Vladimir Radunoviç** invited participants to share their thoughts through the online platform about the weakest link in cybersecurity capacity. It turned out that there were no technological issues among the weakest links, but that human-related factors were predominant (picture 1).

Picture 1: 'Word cloud' of participants' thoughts about the weakest link in cybersecurity capacity.

Mr. Radunoviç went on to present some of the messages taken away from the pre-day workshop, on the possible framework for looking at what GGPs are: 'a practice' could be an activity or set of activities which helps an initiative to reach its goals, 'a global practice' can be implemented on the global scale or replicated in different regional or national settings, while 'a good practice' may stand for a practice proven to have been efficient or effective.

Some of the key questions that need to be addressed in order to help assess what good practices could be, were then shared with the groups to discuss:

What are the existing practices?

- Whose capacity do we want/need to build? Capacity for what?
- What are the challenges to make practices global? How to mitigate those challenges?

14 groups of five to eight people in each were created, each group covering one of the topics of the existing and emerging initiatives:

- cybersecurity culture and awareness raising
- CSIRT/CERT development, communications and maturity
- critical information infrastructure protection
- coordinated vulnerability disclosure
- Internet infrastructure and Internet standards
- maintaining a healthy and 'green' cyber-environment: monitoring threats and increasing prevention capacities
- assessing and developing cybersecurity capability
- cybercrime capacity building
- cybersecurity strategies and action plans
- confidence building measures and international peace and security in cyberspace.

Each group was facilitated by a group moderator, and supported by the representative of the related initiative.

11.30 – 12.30 Plenary: Recap Global Good Practices

During the recap, the group rapporteurs were invited to briefly outline, with regards to the particular initiative:

Up to 3 examples of good practices;

- Up to 3 key stakeholders, and 3 – 5 main capacities for those stakeholders;
- 3 key challenges and at least 1 mitigation measure for each.

Some examples of possible good practices that the tables came up with, include:

- Regarding CIIP, creation of a constantly updated directory of contacts;
- For Cybersecurity Strategies, creation of metrics to measure successful implementation
- For confidence building measures (CBM), coordination of the CBM approach among stakeholders.

Other practices mentioned and discussed in the context of various initiatives included toolkits, training sessions, promotion and sharing of resources, etc. As for the challenges discussed at the roundtables, few examples include: funding, political will, lack of awareness, differences in capacities/ maturity, unwillingness to acknowledge weaknesses, and a lack of expertise.

At the closing, Mr. Radunoviç briefly presented the next steps, which include working directly with the initiatives to assist them to identify their list of GGPs, and to involve the Advisory Board, the GFCE members and the broader community to reflect on the GGPs identified by the initiatives, before presenting them at the GCCS.

13.45 – 14.45 Breakout session: Showcases non GFCE (parallel sessions)

ASEAN Cyber Capacity Programme

Mr. Hoo Ming Ng, Singapore

ASEAN Cyber Capacity Programme (ACCP) was launched by the Singapore government on 11th October 2016 at ASEAN Ministerial Conference on Cybersecurity during the Singapore International Cyber Week. With this S$ 10 million program Singapore strongly recognizes that a secure and resilient cyberspace is an enabler of economic progress and better living standards. States can contribute to the security and resilience of cyberspace by adhering to well-defined and practical voluntary norms of behavior that are supported by robust confidence building measures (CBMs).

What are the broad objectives of ACCP initiatives?

- Raise awareness and foster deeper regional discussions on cyber norms;
- Enhance regional coordination of capacity building and incident response and develop metrics to assess effectiveness in these areas;
- Build regional capacity in strategy development and cyber legislation; and
- Contribute to global efforts on the development of a set of cybersecurity/IoT standards.

Singapore will organize several workshops and conferences in 2017 on a range of cyber topics, obviously with the Singapore International Cyber Week (SICW) from 19th – 21st September as the main event.

CAMP (Cybersecurity Alliance for Mutual Progress)

Ms. You Jin Moon, Korea Internet & Security Agency (KISA)

CAMP is a Global Network Platform launched by the Republic of Korea on 11th July 2016 which currently consists of 53 Members which are government organizations from 40 States. Besides the Chair and a Secretariat, the CAMP Platform consists of an Operations Committee (to contribute to the discussion on formalizing the framework and operation of CAMP) and 3 Working Groups (Policy, Technology and Capacity Building) which seek specific cooperative items for mid and long-term projects.

Key topics for the CAMP platform are:

- Information Sharing (e.g. information security related acts, CERT structure of countries, policies and strategies)
- Capacity Building (e.g. education programs, hosting international conferences, seek and develop international joint projects).

- Joint Response (e.g. sharing threat information, coordination measures in contingencies, joint drills)
- Matchmaking (e.g. connecting relevant agencies and companies, share technologies and people-to-people exchanges).

CAMP has an Annual General Meeting for their members but also organizes Regional Conferences, seminars and trainings aiming to deliver concrete and pragmatic tools and best practices.

NIST Cybersecurity Framework

Ms. Isabelle Roccia, U.S. Mission to the European Union

The U.S. Department of Commerce National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity," commonly known as the NIST Framework, and standards such as ISO 27001 "Information Security Management." NIST developed the Framework through a series of public workshops and feedback sessions.

Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

Initially published in 2014, in early 2017 NIST announced it is in the process of updating the Framework, again using requests for public comment, workshops, and webinars to engage stakeholders. In the three years since its publication, 30% of surveyed U.S. companies have adopted the Framework in some form, with the number expected to grow to 50% by 2020.

STADIA

Mr. Michael Roberts, INTERPOL

Established by INTERPOL in 2012 and funded by Qatar, the aim of Project Stadia is to create a Centre of Excellence to help INTERPOL member countries in planning and executing policing and security preparations for major sporting events.

Michael Roberts started the STADIA showcase off with an introductory video about the start of INTERPOL and how the organization has evolved during the past century. With the use of other short videos, Michael Roberts sketched how Project Stadia organizes annual expert group meetings on the key themes of legislation, physical security and cybersecurity. These meetings bring together global experts from law enforcement, event organizing committees, government, the private sector, academia and civil society to explore state-of-the-art research and analysis and develop independent recommendations for planning and executing security arrangements for major international sporting events.

During an expert meeting in April 2017, some 20 cybersecurity experts from seven countries are reviewing cyber threats and how they impact public safety operations, with a specific focus on: coordinating national cyber incident responses; harmonizing cybersecurity risk management standards across infrastructures at a national level; and, conducting cybersecurity risk management on national infrastructures impacted by major public events.

NRD Cyber Security: Addressing Cyber Resilience

Ms. Akvile Giniotiene, NRD CS

NRD Cyber Security is a cybersecurity technology consulting, incident response and applied research company. NRD companies implement projects in more than 50 countries worldwide.
In the presentation is concluded that a change of mindset is needed:

- Awareness that digitization exposes countries and organizations to additional risks that need to be contained;
- Making sure that a country/ organization is ready to deal with those risks;
- Making cybersecurity an integral part of all digital development programmes.

NRD CS activities focus on:

- Countries' cybersecurity maturity assessments and roadmaps to better cybersecurity;
- Cybersecurity governance framework development;
- Legal and regulatory cybersecurity framework development;
- Law enforcement capacity building;
- Critical infrastructure identification and protection;
- CSIRT establishment and capacity building.

Cybersecurity / Cyber Capacity Building in the ECOWAS region

Dr. Raphael KOFFI, ECOWAS

In the presentation is stated that ICT is key in the development of West Africa and the engine of regional integration. The core objective of the ECOWAS in ICT is the establishment of a single Digital Market in West Africa. A secure cyber environment in the region is an enabler for this Digital Single Market. Therefore, th goal for ECOWAS is to contribute to enhance Cyber security among ECOWAS countries.
The current situation of cyber security / cybercrime is that some ECOWAS countries occupy preeminent positions in global cybercrime ranking. 70% of cybercrimes are related to known vulnerabilities that are not addressed. Further, awareness is still poor and there is a need to establish a Cybersecurity CERT/CSIRT.

In the presentation some challenges are mentioned:

- Domestication: enforcement of laws at the national level; campaigns to sensitize on cyber laws; insufficient legislations.
- Skillset: desperate need of capacity building and a low level of capacities to respond to cybercrime cases.
- Strategies and policies: a lack of national cybersecurity strategies.
- Cooperation: information sharing on best practices and a low level of regional and international cooperation.

Internet Society (ISOC)

Ms. Ceren Unal, ISOC

In the presentation ISOC is summing up 5 elements of their collaborative security approach:

- Fostering confidence and protecting opportunities;

- Collective responsibility;
- Fundamental properties and values;
- Evolution and consensus;
- Think globally, act locally.

In the presentation several example are mentioned:

1. *Mutually Agreed Norms for Routing Security (MANRS*). MANRS is a document and a commitment for a company which subscribes to it
2. *The Deploy360 Programme*. The IETF creates protocols based on open standards, but some are not widely known or deployed. People seeking to implement these protocols are confused by a lack of clear, concise deployment information. The Deploy360 Solution: provide hands-on information on IPv6, DNSSEC, TLS for applications, and Securing BGP to advance real-world deployment. Also, work with first adopters to collect and create technical resources and distribute these resources to fast following networks.
3. *Internet Infrastructure Security Guidelines for Africa*. These Internet Infrastruture Security Guidelines were launched on 30 May 2017 in Nairobi during the Africa Internet Summit. Governments, companies, network operators, universities and organizations across African Union member states are encouraged to take action to implement the Internet Infrastructure Security Guidelines. The guidelines are developed by a multistakeholder group of African and global Internet infrastructure security experts. Goal is to help AU member states strengthen the security of their local Internet infrastructure through actions at a regional, national, ISP/operator and organizational level.

Addressing Supply Chain Risk

Mr. Andy Purdy, Huawei; **Ms. Kaja Ciglic,** Microsoft

The presenters introduce the East West Institute (who cannot be present). EWI is an independent NGO that works to reduce international conflict by addressing seemingly intractable problems that threaten world security and stability. EWI brings together many different stakeholders from expert communities to drive solutions.

Focus of the presentation is the **Buyer's Guide** which aim is to inform buyers about the risks inherent to ICT services. Overarching recommendations of the Guide are:

- Engage in dialogue about risk management
- Use the guide to frame the dialogue
- Rely on international standards to increase confidence in results

The Buyer's Guide names 5 principles that are important for all stakeholders involved in the ICT Supply Chain:

- Maintain an open market that fosters innovation and creates a level playing field;
- Create procurement practices that are fact-driven, risk-informed, based on international standards;
- Avoid requirements that undermine trust (such as back doors);
- Evaluate practices of ICT providers;
- Create tools to address risks.

15.15– 16.15 Plenary: Update regional initiatives

Moderated by **Pablo Castro** (Chile)

Cybersecurity and Cybercerime Trends in Africa

Mr. Ilias Chantzos, Symantec

This is the first completed and fully delivered GFCE initiative. We were able to collect information, based on the Symantec Threat Analytics, send questionnaires to country, get support of the Council of Europe, have the U.S. government function as the catalyst; we were able to produce this report about Africa.

- We learned that it can be done, a model between private and public sector. We learned better to engage in the African context. Collaboration on the project was very gratifying.
- It is important now that the AU has the ball. Important to see after a few years what the progress is on the basis of the report.

CyberGreen

Ms. Yurie Ito, CyberGreen

There is a large base of computers, routers etc., which are vulnerable. With the statistical tool (stats.cybergreen.net) it can be seen how countries are doing on cybersecurity. By doing this, an organization can bolster their security. For example, Singapore used the cybergreen metrics at the ICT ministry and it has helped in the reduction of vulnerabilities.
The tool also shows trends and that encourages improvements. It is very important to include academics to analyze what policy is really improving health.

CyberGreen would like to be a partner in capacity building programs. It can provide data, metrics, training materials, help how to clean up the unhealthy risk indicators. For CyberGreen the GFCE has been a great platform to find sponsors.

Progressing Cybersecurity in Senegal and West Africa

Ms. Petra Nijenhuis-Timmers, the Netherlands; **Ms. Ndeye Fatou Coundoul Thiam,** Senegal

The Awareness Initiative on cybersecurity between Senegal and the Netherlands was launched at the GCCS2015. Its goal is bridging capacity building gaps and raise awareness. The results of the initiative so far are:

- A cyber Capacity Review of Senegal
- An expert meeting within Senegal
- Publications in the Global Magazine on Cyber Expertise
- Setting up a local coordination group on cybersecurity
- Adoption of Senegal National cybersecurity strategy which is to be finalized

Preventing and Combating Cybercrime in Southeast Asia

Mr. Alexandru Caciuloiu, UNODC

4 thematic areas in cybercrime area where UNODC builds capacity:

- Technology dependent crimes (malware etc.);
- Technology enabled crime (internet fraud, scams);
- Online child exploitation;
- Digital evidence.

Within the initiative the first step was assessments visits in several countries. Then, UNODC followed with programs to influence legislative changes to criminalize child exploitation.

UNODC is planning to give support to countries to continually update legislation**.** For example by giving training on tracing Bitcoins. More and more abuse of cryptocurrencies is seen. Further, the aim is to deliver a workshop for the use of social media by law enforcement. Finally, UNODC would like to build digital forensic capabilities for ASEAN members.

Cyber Security Initiative in OAS member states
Belisario Contreras, OAS
OAS focuses on three core activities: policy development, institutional strengthening, research and outreach. Many countries in the region have adopted national cybersecurity strategies: like Colombia, Paraguay. Other countries are in the process of developing a cyber strategy.

Activities of OAS are:

- New working group for CBMs;
- Technical activities relating to CERTs;
- Big activity in Montevideo in the context of the Awareness Month;
- Developing more technical documents with the private sector;
- Strengthening cooperation between tech community and civil society.

All these works are based on collaboration. Resources are very limited, so there for it is important to share resources.

Promoting Cybersecurity Due Diligence across Africa
Johanna Vazzana, MITRE Foundation
This is a joint US-AUC initiative with 2 main objectives:

- Raising political awareness of best practices for a national approach to cybersecurity.
- Reinforcing the building blocks needed for organizing national efforts.

In the presentation several means are mentioned to achieve these objectives:

- Develop a national cybersecurity plan;
- Enhance Government-Private Sector collaboration;
- Modernize laws and policies;
- Develop national incident management capabilities;
- Culture of cybersecurity (for example: sessions, workshops, feedback, activities that help refine and help identify goals, stakeholder mapping, finding resources).

16.15 – 16.30 Plenary: Wrap-up and next steps

GCCS2017

India announced that the GCCS2017 will take place in New Delhi at 23rd and 24th of November.

Process Global Agenda and Global Good Practices:

- July - Sept.: the GFCE community will be involved to develop the first draft of the Global Agenda. Initiatives will be approached to develop a first draft of the Global Good practices. The Secretariat will cooperate in this regard with TNO and DiploFoundation.
- End of sept: discuss the first draft of the GA CCB and the GGP more directly during the Cyber Week in The Hague (physical and remote consultation).
- Sept - Nov.: broader consultation with the GCCS community takes place.
- By the time of the GCCS (23/24 November), the final drafts will first be presented to the GFCE community at the GFCE pre-meeting in India.

Two suggestions came from the audience:

- Produce a “stakeholders map”;
- Publish the amount of investment that has been mobilized for CCB.

The GFCE Secretariat will pick this up as part of the process. The Indian co-chair concluded the Annual Meeting by thanking the EU as a host and the GFCE members and partners for their active participation, resulting in a successful Annual Meeting.

Annex 1 – Workshop Global Good Practices, DAY 0

The morning workshop on 30 May was organised to discuss what a global good practice (GGP) is, and how GFCE can best distil the GGPs of its global initiatives, using experiences from other areas of capacity development. It was attended by some 40 participants: representatives of all the global initiatives, representatives of several international and regional organisations, and interested GFCE members.

The workshop aimed to encourage the representatives of the initiatives and other participants to look at their work using a capacity development lens, applying some of the key concepts and approaches from this field to discuss GGPs. Therefore, the workshop was conceptualised as a blend of presenting capacity development theory and practice from non-cyber fields, plenary discussion on main concepts involved in defining the GGPs, and small group discussions aimed at applying capacity development concepts to work in the cyber field.

David van Duren, head of the GFCE Secretariat, welcomed participants and reminded them of the endorsed GFCE Roadmap that outlines two main deliverables for the Global Conference on Cyber Space (GCCS), to be held in India in November 2017: the Global Agenda for Cyber Capacity Building, and the supporting set of GGPs in capacity building – preferably at least three from each initiative. He also explained the role of DiploFoundation in assisting and facilitating the efforts of the initiatives to identify and outline their GGPs. **Vladimir Radunoviç**, director of cybersecurity and e-diplomacy at DiploFoundation, briefly outlined the planned methodology for work on the GGPs. The process will include mapping the practices of each initiative, reviewing these practices using the framework of capacity development theory and practice, and matching practices against gaps in global cyber capacities. This process should facilitate the work of initiatives to identify their own good practices and to consider if and how these are, or can become, global.

The introductory presentation on capacity development, delivered by Diplo's educational programmes director **Hannah Slavik**, aimed at bringing all participants to a common understanding about key concepts and practices in capacity development from the non-cyber field. Slavik introduced some key definitions of capacity and capacity development (from UNDP, ECDPM, SDC, OECD) and discussed various dimensions including levels, types, themes, and methods and tools of capacity development. Slavik then looked into elements of good capacity development practice: clearly defined aims (e.g. whose capacities should be built and for what), working with relevant stakeholders, adapting practices to the local environment, being responsive and flexible to address emerging needs, building on existing capacities, using a comprehensive approach, measuring results, and ensuring sustainability.

A discussion followed, moderated by Diplo senior associate **Dejan Dincic**, on what the capacities, impact, and good practices would mean in context of the cyber field.

In discussion about GGPs – especially in the context of GFCE global initiatives – the point was raised that one should look into proven good practices, potential good practices, but also bad practices which may be a great way to learn and improve. The Global Counterterrorism Forum (https://www.thegctf.org/) was mentioned as an effective forum which the GFCE might learn from.

A discussion in three smaller groups followed, moderated by Slavik, Dincic and **Tereza Horejsova**, Diplo's project development director. Looking into what are key capacities for the cyber context, the groups identified, among others, capacities for:

- Understanding the terminology specific to the field
- Setting up and improving the work of CERTs, and incident response in general
- Law enforcement authorities to deal with cybercrime and analyse digital evidence
- Digital hygiene and building cybersecurity culture
- Increasing political will and awareness about cybersecurity
- Risk management
- Strategic planning and setting priorities
- Measurement of impact, and especially global consequences
- Cross-sectoral cooperation
- Building trust, including through creating a policy framework to support this
- Adaptability and sustainability, with regards to political changes in governments
- Developing human resources – institutional, and on individual levels
- Education to build capacities

It was particularly emphasised that only a holistic approach to capacity development can create impact, rather than developing individual sets of capacities. In this regard, it was suggested that while it is important to identify specific capacities in order to be able to prioritise action plans, it is of utmost importance to also look at the interdependence of various capacities.

The discussion about planning for impact and using monitoring and evaluation tools for the initiatives was particularly diverse and useful, bringing up important ideas, challenges and specific suggestions for the GFCE. Important ideas included:

- clear aims and objectives are needed before monitoring and assessment of impact can be conducted (e.g. beneficiaries, goals, etc.)
- We should look into what are the financial and social consequences of our actions
- Tangible goals and clear objectives should be set
- Meaningful indicators should be developed to show impact on the larger scale
- Baseline measurements need to be established; they should be specific for each initiative, but also coordinated among initiatives to avoid replication of measurements
- Developing a set of common standards could lead to developing tools for measurement
- Available data sets can be used for measuring baselines: big data, or hopefully big open data
- Donor-driven initiatives should already have monitoring and evaluation parameters incorporated, which can be used
- Beneficiaries should be invited to measure the impact, through agreed tools
- Funding, which sets priorities, should be aligned with expected impacts and matched with achieved results

Challenges identified with regards to assessing the impact include:

- It is hard to measure political (non-technical) impact
- There are often limited resources to do assessment
- There is a lack of common standard terms and definitions and common language

The question was also raised if there is a value in finding monitoring and evaluation tools to be able to determine the success of GFCE initiatives.

With regards to the GFCE specifically, suggestions were made that initiatives should have some elements of a common approach. This would include to more clearly define what it means to be a GFCE initiative in the future, and assist this process with preparing some sort of GFCE guidelines on components that initiatives should have (such as clear objectives, tangible goals, target stakeholders, evaluation mechanisms, funding transparency, etc.). In this regard, the suggestion was made that the GFCE can discuss establishing common metrics to measure the impact of initiatives in the future. In addition, the GFCE could be a platform for cooperation with the private sector and governments to exchange and/or use big data for measuring impact.

In the final round, the participants discussed some global good practices (or candidates for) from the work of initiatives and similar projects and activities. Some possible GGPs were mentioned, such as the exchange of views among policy makers, industry, and ethical hackers on a framework for coordinated vulnerability disclosure, a toolkit and a training package on how to start with critical information infrastructure protection (CIIP), and a CIIP directory to let parties know whom to contact in case of problems. It was also noted that an informal open voluntary forum for information sharing, based on face to face contact, is a global good practice itself, and Meridian was noted as one such example. A more in-depth look at the good practices of the initiatives was left for the discussion on the second day of the Annual Meeting, together with other members of the GFCE.

Annex 2 – Workshop on Sharing Experiences on Cyber Capacity Building, DAY 0

The afternoon workshop was organized to exchange regional experiences with cyber capacity building (CCB) and identify common experiences, practices and values. Attention was also drawn to how the GFCE community can turn sharing experiences into building new capacities.

Tjarda Krabbendam from TNO (the Netherlands Oganisation for Applied Scientific Research) and **Vladimir Radunoviç** (DiploFoundation) identified the needs in CCB, mentioning:

- Awareness raising
- Combating cybercrime and terrorism
- Incident response
- Technical assistance (broader than incident response, incl. internet infrastructure)
- National frameworks
- Sustainability of capacity building (incl. creating of trusted communities)

They concluded these needs serve as an encouragement to further discuss needs in connection with the available experience at the regional level.

Lara Pace from the Global Cyber Security Capacity Centre (GCSCC) elaborated on the dimensions of a country's cyber security maturity, and identified lessons learned from the work that the GCSCC has done on this. The GCSCC has developed the Capability Maturity Model (CMM) to gather experiences around the world re: CSCB (Cybersecurity Capacity Building). The CMM is trying to create common standards when it comes to CSCB. Lara Pace called upon the audience to think more strategically about 'the way in which we invest' – to inform the global discussion with regional initiatives. She identified two important challenges to CCB:

- They are restricted by (a lack of) political mandate, which prohibits a perfectly comprehensive approach;
- Lack of resources.

Following was a panel discussion with project leads of regional CCB projects. **Alex Caciuloiu** (UNODC), **Zoltán Préscényi** (SYMANTEC) and **Alison August Treppel** (OAS) gave their view on the current major challenges in CCB and the cybersecurity playing field.

Current major challenges in CCB:

- No OAS country is in full cyber maturity, aside from US and Canada, due to lack of resources. There is a lot of work to be done in many areas. Only 6 members have a national cyber security strategy and only 5 have a cyber command and control center.
- The countries with the densest IT infrastructure will have the highest cybercrime. For that reason priorities are very different between many countries. Taking lessons learned from one country and applying it to the next, proves therefore sometimes difficult.

- Major challenge is huge difference in terms of economic development. In some countries there is not enough awareness, especially in lesser developed countries in which there is less reliance on IT infrastructure.

Cybersecurity playing field:

- Events such as WannaCry raised the profile of cybersecurity recently, as opposed to a few years ago. A cybersecurity strategy is the roadmap to realize the greater need for it. We are a small team of 6-10 – even such a team can have a great impact on an entire region.
- There has been a huge shift. The main question used to be: what technology can we use to increase security? Today, I see more awareness about three other greatly important means: people, process, and policy. Consciousness is growing but there is great discrepancy between countries. When governments change, progress can also be scrapped off the table.
- It's important to be in touch with the region. We are trying to push ASEAN and work with them, so that we can try to avoid situations in which a change of government can undo good work. We've recently managed to help introduce legislation.
- CCB is a huge area – ranging from training to internet infrastructure. Therefore we have to work together and share expertise. There is a shortage of qualified personnel and also a shortage of women.
- We should assume that any tech will be hacked and we should always prepare for that. It's difficult because you prepare for known threats and not so much unknown threats.
- Segregated countries mean a borderless operation area for cybercriminals, given legal and political mandates. We are always surprised by the ingenuity of cybercriminals.
- We should also focus on Africa as a 'test bed' for certain crimes, such as SMS fraud which was huge in Africa 5 years ago and now is proliferating elsewhere.
- In a lot of countries there is a high need for the basics, such as awareness. Technology is of course a double edged sword and law enforcement is always behind in this arms race. However, government has limited resources; we have to spend it on known threats.

After the panel discussion, all participants were divided in groups for a table discussion on their local experiences and the lessons that all those attending, and the GFCE community more broadly can learn from these. The main reoccurring observations are captured below:

- International cooperation in global or regional forums such as OAS has been a great help.
- International standards are a useful guide for the implementation in different states when it comes for example to enacting policies with regards to cybercrime training. The Council of Europe has standards in this regard.
- A comprehensive approach, a strategic vision, is necessary.
- Funding is always a problem; one of the key elements of CCB is political will. A 'steering committee' to implement measures is important. Low-cost campaigns, such as awareness on upgrading your firewall, can also be a solution.
- You can have perfect legislation, but at times the public is unaware of this legislation. There needs to be a law enforcement follow-through.
- It is essential to develop instruments, workshops, cooperation centers, etc., to generate a multistakeholder approach and to build trust.

- Invest in sustainability: the trainers need to be trained! Thereby knowledge is retained, which will generate long term effects.
- National points of contact for clear communication lines.