

GLOBAL CYBER EXPERTISE MAGAZINE



**The African Union
Cybersecurity Expert
Group (AU-CSEG)**

-page 26-

**Interview: Strategic
role of MISIP**

on the regional
exchange information
model used by
CSIRT Americas

-page 38-

**The GFCE meets
the Pacific**

-page 42-

**Interview: Miguel
González-Sancho**

on Europe's Digital
Single Market and
Cybersecurity

-page 50-

**INTERVIEW:
CHRIS PAINTER**

President of the GFCE Foundation Board

-page 14-

Editorial

5 Years of the GFCE

- 4 Charting the 5-year growth of the GFCE
- 10 GFCE key deliverables after 5 years
- 12 Insights from the Community: the added-value of the GFCE
- 14 Interview: Chris Painter, President of the GFCE Foundation Board

Global Developments

- 18 Stakeholder engagement in cyber capacity building – lessons learned after 5 years of GFCE
- 22 Capacity building in the UN cyber-deck: The winning card?

Regions

Africa

- 26 The African Union Cybersecurity Expert Group (AU-CSEG)
- 30 Interview: Cheik Bedda on AU's Digital Transformation Strategy

Americas

- 34 Bridging the gender gap in cybersecurity
- 38 Interview: Strategic role of MISIP on the regional exchange information model used by CSIRTAmericas

Asia & Pacific

- 42 The GFCE meets the Pacific
- 46 Online capacity building on cyber law, cybercrime investigation and digital forensics under the Digital India Program

Europe

- 50 Interview: Miguel González-Sancho on Europe's Digital Single Market and cybersecurity
- 54 EUCyberNet – the new kid on the EU cyber capacity building block

Editorial



On behalf of the Editorial Board, I am pleased to welcome you to the seventh edition of the Global Cyber Expertise Magazine! This special edition was originally intended to be presented at the GFCE 5th Anniversary Meeting celebration in the Hague. However, due to circumstances beyond our control, we have launched this edition during our online GFCE V-Meeting 2020 instead.

The Global Cyber Expertise Magazine is a joint initiative by the African Union, the European Union, the Organization of American States and the Global Forum on Cyber Expertise. The Magazine aims to provide cyber policymakers and stakeholders insight on cyber capacity building projects, policies and developments globally.

As we celebrate our 5th Anniversary in April 2020, this edition features a unique “5 years of the GFCE” segment, looking back at what we have achieved thus far, what is next, and what the added value of the GFCE is. Our cover story is an interview with Mr. Chris Painter, President of the GFCE Foundation Board, who shares his perspective on the path forward for the GFCE.

From the global developments section, one article from members of the GFCE Advisory Board looks at the importance of civil society actors in cyber capacity building. Another article explains that capacity building could be a possible common denominator in the complex UN-level discussions (GGE/OEWG).

From Africa, the African Union Commission shares their efforts to tackle cybersecurity concerns from a multi-stakeholder perspective with the formation of an African Union Cybersecurity Expert Group. Also, read about the African Union's new Digital Transformation Strategy and why a regional approach is necessary in an interview with Mr. Cheikh Bedda.

From the Americas, the Organization of American States emphasizes the need to bridge the gender gap in cybersecurity and ICT. An interview on the strategic role of the Malware Information Sharing Platform (MISP) provides insight on the regional model used by CSIRTAmericas.

From Asia/Pacific, read more about the GFCE's inaugural regional Pacific Meeting that took place in February 2020 as well as India's online cyber capacity building program for law enforcement agencies and judiciaries.

From Europe, an article on the new EU CyberNet initiative explores what makes this project unique and how it could support the EU's ongoing efforts in cyber capacity building. Also, an interview with Mr. Miguel González-Sancho gives insight on the work of the European Commission's “Cybersecurity Technology and Capacity Building” Unit.

We thank our guest writers for their valuable contributions to the seventh edition of the Magazine and we hope you enjoy reading the Global Cyber Expertise Magazine!

On behalf of the Editorial Board,

David van Duren

Director of the GFCE Secretariat

CHARTING THE 5-YEAR GROWTH OF THE GFCE

Written by: Kathleen Bei, Advisor, GFCE Secretariat

2020 is a special milestone for the GFCE as it celebrates its fifth anniversary on 16 April and is now officially established as a GFCE Foundation. Committed to its mission to strengthen cyber capacity and expertise globally through international collaboration, the GFCE has met many achievements during these five years, building a strong foundation and community to support cyber capacity building globally and position itself as the international coordinating platform on cyber capacity building. A key element of these successes is the active engagement and involvement of the community. Looking ahead to 2022, the GFCE aims to further strengthen the GFCE ecosystem by improving processes, expanding work methods, growing the community and encouraging active engagement, establishing its regional presence and organizing more meetings around the world.

The GFCE is born

This April marks an important and exciting milestone for the Global Forum on Cyber Expertise (GFCE) as it celebrates its fifth (5th) anniversary. The idea of a platform to share cyber expertise for global cyber capacity building was born from discussions at the 2015 Global Conference in Cyber Space (GCCS) in the Hague; resulting in 42 ministers and high-level representatives from business and international organizations to endorse the establishment

of the GFCE on 16 April 2015. With a vision that every citizen of the world may fully reap the benefits of ICT through a free, open, peaceful and secure digital world, the GFCE was launched to strengthen cyber capacity and expertise globally by being a pragmatic, action-orientated and flexible platform for international collaboration.

The GFCE continues its efforts to turn this vision into reality and stays actively committed to its mission, recognizing that strong cyber capacity and exchanging expertise is needed not

just for the progression of digital security but also for economic and social development. Today, the GFCE is the only platform that coordinates global cyber capacity building, reducing the duplication of efforts in the cyber capacity building ecosystem while maximizing expertise and resources available. This is carried out through the GFCE Working Groups, Cybil Knowledge Portal, the Clearing House function, practical GFCE initiatives, and the establishment of the GFCE Foundation.

More stakeholders from all regions of the world are recognizing the value of the GFCE as evident in the growth of the community to over 115 members and partners from governments, international organizations, non-governmental organizations, civil society, private companies, the technical community and academia. As a community-driven platform, the GFCE is able to thrive because of its strong foundation and expansive network, which was a key focus of the GFCE in its formative years of 2015 – 2017.

GFCE Initiatives

In the first two years, the work of the GFCE was organized around regional and global initiatives. As a bottom-up platform, members and partners could choose what they wish to initiate, collaborate on, and/or provide specific expertise. As a deliverable of these initiatives, a set of GFCE global good practices (GGP) would be developed.¹ By sharing best practices and lessons learned, the GFCE aimed to improve cyber capacity building efficiency and effectiveness.

To include and amplify civil society involvement in the GFCE, the first GFCE Advisory Board was installed in 2016, comprising of civil society representatives. Before introducing new ideas or work methods to the GFCE community, the Secretariat first proposes the ideas to the Advisory Board for review. The Advisory Board provides constructive feedback and strategic advice, while ensuring a multi-stakeholder approach to the GFCE's work.

Setting the Global Agenda and the GFCE Working Groups

One of the turning points for the GFCE was the 2017 GCCS in New Delhi, where the GFCE put forth and received support for the [Delhi Communiqué](#) on a Global Agenda for Cyber Capacity Building. This was significant because receiving endorsement on a high political level provided the necessary political impulse for recognizing the importance of cyber capacity building. Furthermore, developing a Global Agenda was crucial in order to determine priorities and methods for implementation in 2018 and beyond. By developing the Agenda, the GFCE effectively shifted its focus in 2017 to position itself as the platform for exchanging cyber expertise and coordinating global cyber capacity building efforts.

Building on the global good practices identified through GFCE initiatives, the Global Agenda prioritized five themes and eleven topics, calling for action to jointly strengthen cyber capacities globally. The entire GFCE community endorsed the [Delhi Communiqué](#), which was essential not only to coordinate global efforts but also, to encourage multi-stakeholder dialogue on its implementation.

As a first step towards concrete action on the implementation of the Agenda, a new structure in the GFCE was established – the GFCE Working Groups. In the Working Groups, Members and Partners work together and collaborate on topics that fall under the Group's broad theme, as prioritized in the [Delhi Communiqué](#). These themes are: Cyber Security Policy and Strategy, Cyber Incident Management and Critical Infrastructure Protection, Cybercrime, Cyber Security Culture and Skills, Cyber Security Standards.

Today, the Working Groups delivers the GFCE’s mission by being the engine and lifeforce of the GFCE, involving over 85% of the Community. For coherence and synergy, the work and common deliverables of all Working Groups are divided across the same four pillars: Coordination, Knowledge sharing, Clearing House and Cyber Capacity Building Research Agenda. Each of the pillars have been derived from the GFCE’s overall strategy as illustrated below.

Cybil Knowledge Portal

Under the coordination and knowledge-sharing pillars of the GFCE Working Groups, Members and Partners share their cyber capacity building projects and recommend tools, frameworks, guides, publications etc. To consolidate this information in one place and make this more accessible to the wider cyber capacity building community, in line with the GFCE’s efforts to support

cyber capacity building globally, the idea to develop an online Cyber Capacity Building knowledge portal was conceived. In October 2019, the GFCE launched the Cybil Knowledge Portal (www.cybilportal.org) together with knowledge partners that form the Portal Group - NUPI, GCSCC, FIRST, DiploFoundation and ASPI. Since its launch, new features of Cybil include an events calendar with information on upcoming cyber capacity building conferences, workshops and

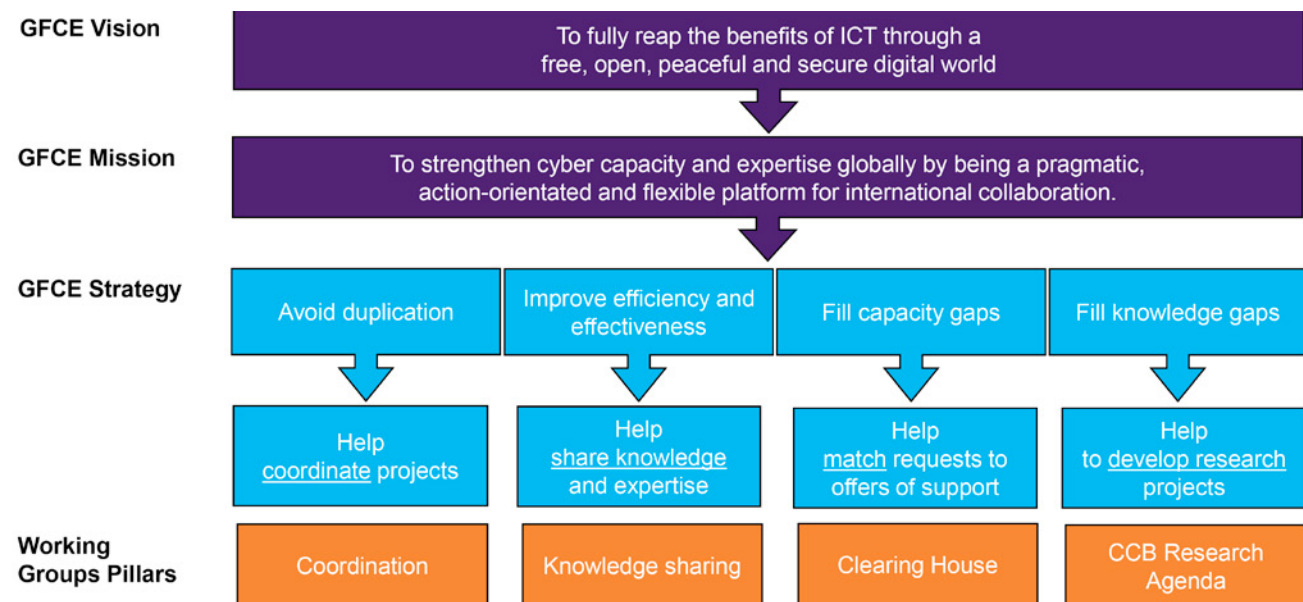


Figure 1. The GFCE’s vision, mission and strategy, and how this links to the Working Group pillars.

“The GFCE continues its efforts to turn this vision into reality and stays actively committed to its mission, recognizing that strong cyber capacity and exchanging expertise is needed not just for the progression of digital security but also for economic and social development.”

meetings around the world. As of March 2020, Cybil contains 500 projects, 72 tools, 74 publications, 421 actors and 39 upcoming events. The content is identified and updated by the GFCE community through the GFCE Working Groups.

Clearing house

Recognizing that cyber capacity building can never be a one-size-fits-all model and that tailored assistance to local contexts is a determinant of successful capacity building projects, the GFCE seeks to be a capacity building clearing house. Through the GFCE Working Groups, the GFCE plays a ‘match-making’ role; effectively matching country, private sector and civil society donors and implementers that can provide key capacity building services with countries that request assistance. Through this process, the GFCE is currently helping Sierra Leone with their National Cyber Security Strategy, Senegal with setting up a CSIRT (Computer Security Incident Response Team) and The Gambia with Cybercrime Legislation. In October 2019, the GFCE also facilitated the first West Africa coordination meeting to enable members and partners working in the region to discuss projects, deconflict work and identify challenges and opportunities.



Figure 2. The Gambia raised its Clearing House request during the Cybercrime Working Group side-meeting during the 2019 Octopus Conference in Strasbourg.

“By developing the Agenda, the GFCE effectively shifted its focus in 2017 to position itself as the platform for exchanging cyber expertise and coordinating global cyber capacity building efforts.”

Cyber Capacity Building Research Agenda

In discussing the challenges faced by the GFCE community, it became increasingly clear that knowledge gaps existed and the GFCE could potentially address these gaps. To help the capacity building community design and run effective projects, a new pillar of the GFCE Working Groups was thus introduced in 2020. Through the Working Groups, knowledge gaps and research that would be useful and that may help the community achieve their strategic and operational goals are being identified. The GFCE is collecting and prioritizing these research needs into a Global Cyber Capacity Building Research Agenda. This also responds to the call of the GFCE Community for a flexible mechanism that would help them identify common research requirements and generate targeted research relevant to ongoing GFCE work and Member’s activities. The Advisory

Board has taken the lead on developing this idea into a clear process; with the formation of the GFCE Research Committee as the first actionable step.

GFCE Foundation

In December 2019, the GFCE embarked on its transition into an independent, not-for-profit GFCE Foundation. With a new entity added to the GFCE, an international Foundation Board, the Foundation is a vehicle that enables the GFCE to grow sustainably, become even more internationalized and accept funding from multiple donors. It provides a new channel for countries to support global cyber capacity building by supporting the core activities of the GFCE and the functions of the GFCE Secretariat, which is necessary for the GFCE to achieve greater success and fortify its position as the global coordinating platform for cyber capacity building.

Towards 2022

For the next two years, the aim is to continue strengthening the GFCE ecosystem by improving processes, expanding work methods, growing the community, and organizing more meetings around the world. The GFCE also hopes to improve regional coordination and strengthen its regional presence on different continents through the GFCE regional coordination meetings introduced in 2020.² However, the success of the GFCE as a global coordinating platform on cyber capacity building relies on the buy-in of all governments around the world and the GFCE community actively voicing their

capacity needs and sharing expertise. Together with the GFCE Foundation Board, the GFCE Secretariat looks forward to drive momentum for realizing GFCE's vision and mission by encouraging active engagement of the GFCE community, receiving funding from multiple donors and demonstrating its added value to those outside the community.

“As we charge forward towards 2022, we emphasize that a key element to the success of the GFCE is and will always be our strong community – their active participation and engagement as well as support makes it possible to realize our vision and mission.”

To get there, 2020 will be an important inflection point for the GFCE as it celebrates its fifth anniversary and is now a GFCE Foundation, opening the door to many possibilities for sustained growth. During the 7-week online GFCE V-Meeting, we will recognize our achievements thus far and engage the GFCE community on the way forward.³ The community will have the opportunity

NOTES

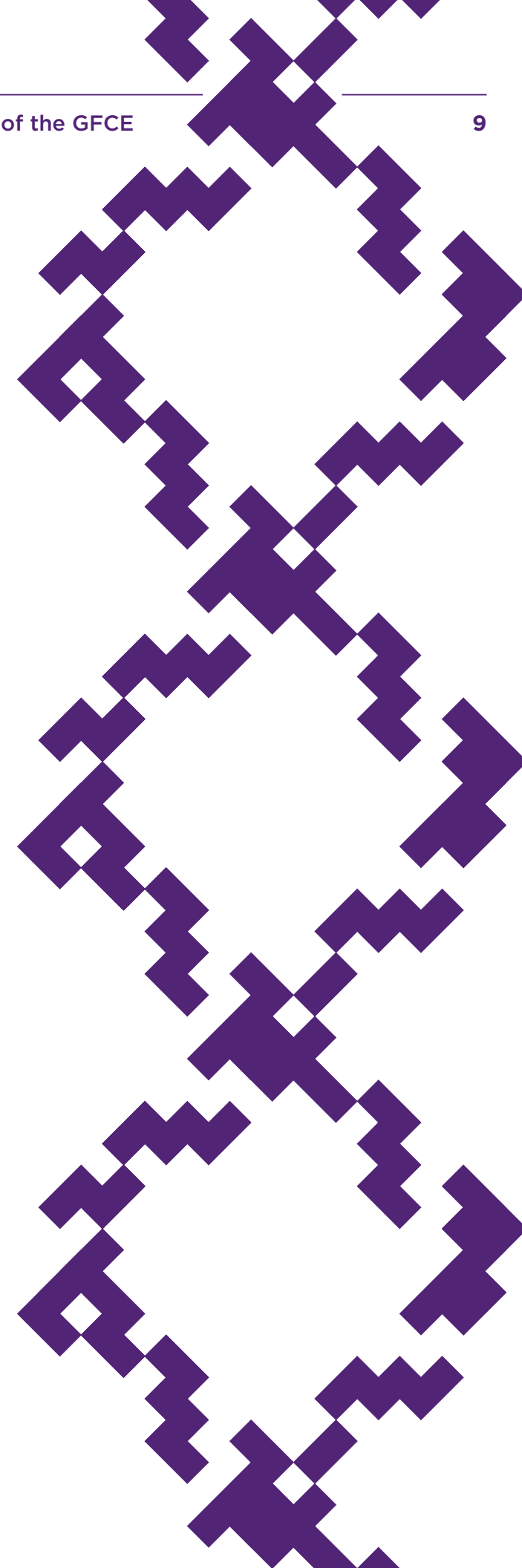
2

Regional Meetings are planned for the Americas, Africa and Southeast Asia and have already been held for Europe and Pacific in 2020. More information on the Pacific Regional Meeting can be found on page 42 of this Magazine, “GFCE meets the Pacific”.

3

The “V” signifies both the roman numeral ‘five’ (as we celebrate our fifth anniversary) and ‘virtual’ (as the sessions are online).

to participate in sessions divided across different tracks: GFCE Members and Partners content, GFCE projects and processes, and GFCE Roadmap 2022. More notably, the GFCE community will be able to provide input on the GFCE's big questions for the drafting of the Roadmap 2022, interact with the new Foundation Board, and provide comments and suggestions on the GFCE clearing house mechanism being developed. Steps towards establishing a Research Committee will also be taken during this period and a clear process for the global cyber capacity building Research Agenda will be developed and implemented to fill knowledge gaps and needs. As we charge forward towards 2022, we emphasize that a key element to the success of the GFCE is and will always be our strong community – their active participation and engagement as well as support makes it possible to realize our vision and mission.



GFCE key deliverables after 5 years

GFCE FUNDING OPPORTUNITIES



CONTRIBUTIONS TO GFCE PROJECTS AND ACTIVITIES

NETWORK

42
↓
116
MEMBERS & PARTNERS



INITIATIVES

9
↓
21
GLOBAL AND REGIONAL INITIATIVES (CCB PROJECTS) UNDER THE GFCE UMBRELLA



GLOBAL AGENDA

ENDORSEMENT OF THE DELHI COMMUNIQUÉ BY THE ENTIRE GFCE COMMUNITY



PRIORITIZING 5 THEMES AND 11 TOPICS ON CYBER CAPACITY BUILDING



EVENTS

50+
GFCE MEETINGS ALL OVER THE WORLD



WORKING GROUPS

IMPLEMENTING THE DELHI COMMUNIQUÉ



5 THEMES



BRINGING MULTI-STAKEHOLDERS TOGETHER




COORDINATING GLOBAL CCB EFFORTS ON THE RESPECTIVE TOPICS



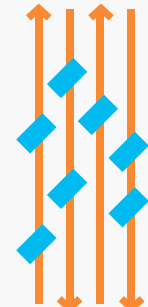
ONLINE PORTAL

LAUNCH OF CYBIL, THE CCB KNOWLEDGE PORTAL




PRACTICAL CCB-RELATED INFORMATION:

- PROJECTS
- TOOLS
- PUBLICATIONS
- ACTORS
- EVENTS




CLEARING HOUSE

5 COUNTRIES HAVE REQUESTED THE GFCE WORKING GROUPS



SUPPORT WITH NATIONAL CYBERSECURITY STRATEGIES, CSIRTS OR CYBERCRIME LEGISLATION



FOUNDATION

LAUNCH OF THE GFCE FOUNDATION



GUARANTEE CONTINUITY, SUSTAINABLE GROWTH AND INTERNATIONALIZATION OF THE GFCE



Insights from the Community: the added-value of the GFCE

Sandra Sargent

Senior Digital Specialist,
World Bank



“GFCE has brought tremendous value by connecting us with other partners in the cybersecurity field. I would specifically like to highlight the role GFCE played in coordinating cyber programs in Africa. In addition to holding joint Africa coordination meetings, GFCE helped establish platforms for collaboration, providing data analytics on cyber maps in Africa and fostering a lasting friendship among the international community. Addressing cyber threats is a collective responsibility and GFCE has played an important role in bringing all of us together to tackle the challenge.”

Sanusi Drammeh

Principal ICT Officer, MOICI,
The Gambia



“The GFCE provided The Gambia an opportunity to connect, network and contribute to the global cyber capacity building community. The GFCE is also facilitating the Gambia’s Clearing House request by playing a matchmaker role and plays an instrumental role in informing the Gambian Representatives on global expertise and developments. This positively impacts how the Gambian Representatives are leading and coordinating cybersecurity activities in the Country. Some of those activities include updating the National Cybersecurity Policy, Strategy and Action Plan (currently open for public comments), validating the Cybercrime Bill, and establishing the GM-CSIRT.”

Carolyn Weisser Harris

Lead International Operations,
Global Cyber Security
Capacity Centre (GCSCC)



“Through the GFCE and its community, we and our regional partners have a better understanding of what is happening where and when in cyber capacity building globally. It has enabled us to not only better coordinate the CMM assessments with the activities of other actors, but also disseminate the learnings from the CMM reviews beyond the groups involved in the assessments. This hopefully contributes to the programming of activities by actors in the field and has contributed to the impact of the CMM worldwide.”

Cesar Moline

Director of Cybersecurity,
eCommerce & Digital Signatures,
INDOTEL,
Dominican Republic



“The Dominican Republic is committed to having an open, safe and resilient cyberspace. We have a long history of international cooperation and assistance in matters pertaining to securing cyberspace. That is why for us it was very important to become a member of the GFCE. This has allowed us to not only have access to a multi-stakeholder platform, but also learn from the good practices and experiences of the community and GFCE initiatives. Additionally, it has permitted us to present our national context and how as a country we have thin bureaucratic lines between agencies and agile organizational and procedural frameworks. This enables collaboration and trust on a national and international level, and a true whole-of-nation approach to cybersecurity and capacity building. This experience is what we look forward to sharing through the GFCE with other countries and regions.”

Insights from the Community: the added-value of the GFCE

Andrew Dinsley

Head of Programs – Cyber
Security, UK Foreign &
Commonwealth Office



“When designing our incident response project for Commonwealth partners, we used the GFCE to get ideas for the design and unexpectedly found implementing partners too. When running our projects with Sierra Leone, we found the clearing house process useful for cementing political will and coordinating with other projects. Finally, when working with the Oxford Global Cybersecurity Capacity Centre (GCSCC) to offer national capacity reviews, we found the GFCE useful for sharing the model and the results of the project. We look forward to continuing to work with the GFCE and delivering better projects as a result.”

Yurie Ito

Executive Director,
CyberGreen Institute



“GFCE has partnered with CyberGreen since its establishment. This partnership has allowed CyberGreen, a small size NPO, to feel like we have a super powerful and efficient global outreach team. The GFCE secretariat is always providing invaluable support in accomplishing missions and engages us to truly make an impact. I really appreciate GFCE’s inclusiveness and agility in moving things forward quickly. This is a platform where we can actually make things happen. Whenever we have potential game-changing ideas we like to bring them to GFCE.”

Belisario Contreras

Manager of Cybersecurity
Program, CICTE, Organization
of American States (OAS)



“When the GFCE was proposed during the 2015 Global Conference on CyberSpace (GCCS2015) in the Hague, it was a concept never before witnessed for cybersecurity. The recognition of capacity building as a strategic method to combat emerging cyber threats resonated with the OAS for almost two decades; we had approved a regional cybersecurity strategy and a Cybersecurity Program was established to focus on building cyber capacities and capabilities within OAS Member States. As such, from our perspective, the GFCE is an excellent interlocutor between States and the private sector in the provision of the needed resources and technical capacity, as we strive to improve global cyber resilience. We have had a great working relationship with the GFCE over the years and look forward to the work of the Foundation in the years to come.”

Yoon-Hoo Kim

Director of Cybercrime
Investigation Division,
Korean Supreme Prosecutors’
Office (KSPO)



“The KSPO is establishing the APC-Hub in collaboration with the GFCE and World Bank, which will facilitate and coordinate the delivery of regional training and capacity building initiatives by various organizations (including many members of GFCE’s Cybercrime Working Group). As the GFCE and the Hub have a shared ethos - avoid the duplication of efforts and maximize efficiency of project delivery - it is expected that the GFCE will be valuable in sharing cybercrime members’ expertise on running existing capacity building projects, support the dispatch of instructors and develop textbooks for cybercrime capacity building training.”

Interview

CHRIS PAINTER, PRESIDENT OF THE GFCE FOUNDATION BOARD

Written by: GFCE Secretariat

Mr. Chris Painter was appointed President of the GFCE Foundation Board during the Foundation's launch in December 2019. Chris has actively contributed to the GFCE since 2018, serving as Chair of the Working Group on Cybersecurity Policy and Strategy (WG A) until he came into his new position. He also serves as a Commissioner on the Global Commission on the Stability of Cyberspace (GCSC) and is a globally recognized leader and expert on cybersecurity, cyber policy, cyber diplomacy and combatting cybercrime. Mr. Painter has been on the vanguard of US and international cyber issues for over twenty-five years and was the world's first top cyber diplomat at the State Department.



Figure 1. Chris Painter representing the GFCE at the OEWG Intersessional Meeting in December 2019.

Q: What are the key elements to successful cyber capacity building?

A: To be successful in building cyber capacity, it would be essential to consider the following elements:

1. If the need for cyber capacity building is only recognized at a working level, it puts a limit on what can be achieved. As such, political engagement is required to ensure that the need for building capacity is a high-level priority for a country.
2. Coordination is essential to reduce overlap (i.e. several entities conducting the same training in the same

place) and increase effectiveness of projects. The GFCE was established particularly to fill the very necessary role of international coordinator to avoid the duplication of efforts while maximizing resources available.

3. Involving multiple stakeholders for collaboration is crucial because there are many different facets to consider that require different expertise (e.g. institution building, establishing a CERT, national strategy adoption, etc.).
4. Tracking a project's progression over time is important, so there needs to be some way to measure success or even gaps. By identifying what is not working, it provides the opportunity to go back and re-address the issue for more effective projects.

In sum, you will need an organized campaign for capacity building that is strategic, comprehensive, not episodic, prioritized politically by the country that seeks capacity building, well-coordinated amongst various providers (donors and implementers), and that involves multiple stakeholders.

Q: What are the challenges in the coming years?

A: We have seen a growing demand for cyber capacity building in recent years; this is predicted to continue in an upward trend in the years to come. Most countries around the world have already recognized that they need some form of capacity building on a broad range of things, so one part of the challenge will be diagnosing what exactly those needs are. Cyber assessments are therefore an important tool for those looking to run cyber capacity building projects to determine priorities and develop an action plan.

A bigger challenge we face is obtaining the resources to meet those

needs and allocating resources to maximize effectiveness. A long-term action plan for every country that is asking for assistance should ideally be developed along with a metrics of success to address this challenge. This requires a combination of efficient organization, multi-stakeholder input, the expertise of several 'expert' parties, other sources of knowledge, as well as the necessary funding. Achieving a combination of these various aspects has not been much of a focus in the past but this is where the GFCE may come in and demonstrate its added value, through its facilitating and organizing functions.

Q: Why was the establishment of a GFCE Foundation important?

A: To ensure that the GFCE can grow sustainably in the long term and become truly international, the creation of a GFCE Foundation was crucial in a couple of ways. First, the Foundation is a vehicle that allows the GFCE to become an even stronger international effort; internationalizing the GFCE Secretariat further and making it possible to address various concerns across continents. Second, it allows us to be more strategic in the long term as we begin charting a new course. Our strategic direction will be informed by the GFCE community, and the GFCE "V" Meeting will be the first opportunity for Members and Partners to provide input on the GFCE's way forward. Third and most importantly, it allows us to gain greater resources as we are now able to draw support from countries and other stakeholders in ways that we were not able to do before due to the structure. The GFCE Foundation therefore makes the GFCE more effective because more parties will have a stake in the result; implying a higher level of accountability. This enables further involvement and commitment of the community to help steer where the GFCE is going, opening

the door to a vast range of possibilities. With the Foundation as a flexible and adaptable mechanism that strengthens the support and facilitation of the GFCE community, I believe we can bring the GFCE to the next step.

Q: Where do you see the GFCE in 2 years?

A: We are currently at a point where the GFCE as a coordinating platform for cyber capacity building is starting to mature and make an impact; we need to take this to the next level. In the next 2 years, I foresee the GFCE growing much larger, not only in the size of its community but also in terms of practical projects and achievements. Some of these achievements include:

- Worldwide recognition that the GFCE is the international platform for the coordination of cyber capacity building around the world, in cooperation with relevant entities and existing mechanisms.
- Championing the necessity to place cyber capacity building higher on the political agenda and establish a truly global cyber capacity building program. We will work towards a high-level global conference in 2021 to bring everyone together; making a difference with resources, focus and cooperation.
- Advocating that cyber capacity building be recognized as a key and necessary element for countries as part of their development and as such, be included in the larger digital or development agenda.
- Playing a major role in developing the Cyber Capacity Building Research Agenda to identify knowledge gaps and develop a global mechanism with an international cyber capacity building fund to fill such gaps through research.

- Performing our clearing house function routinely and responding to requests for assistance quickly and efficiently.

Through the GFCE's efforts today to strengthen the GFCE ecosystem, the GFCE can show international leadership in global capacity building in the years to come.

“With the Foundation as a flexible and adaptable mechanism that strengthens the support and facilitation of the GFCE community, I believe we can bring the GFCE to the next step.”

Q: What should we focus on to get there?

A: One of the priorities would be ensuring that all Members and Partners are engaging and contributing to their full potential. The GFCE community itself plays a key role in driving the successes of the GFCE so it is vital that everyone feels they are involved and interacting with the platform as this maximizes the value of being part of the community.

I also see a lot of value in engaging private companies as they can share their knowledge and resources on cyber capacity building projects from a global responsibility perspective. Additionally, the GFCE community would benefit from the participation and input from the private sector as they can help us to understand and address the impact of emerging technologies on cyber capacity building.



Figure 2. The GFCE Foundation Board with Uri Rosenthal (second from left), Special Advisor to the Board.

Another focus is to establish a strong regional presence in different continents, which is necessary if we want to truly be an international platform as this contributes to efficient coordination on a global level. This year, we introduced regional coordination meetings and we are cooperating with more regional organizations and countries to appoint more GFCE regional liaisons.

“Through the GFCE’s efforts today to strengthen the GFCE ecosystem, the GFCE can show international leadership in global capacity building in the years to come.”

As a community-driven platform, the GFCE needs to continue to be open and flexible to new ideas and encourage the community to be critical. The online V Meeting provides an important opportunity for us to work with the commu-

nity to evaluate our progress and ask: Are we going in the right direction? Are there other things we should be doing? Are there other avenues or opportunities we should be following? Are there things we’re doing that don’t make sense? The community’s response to such questions would be useful in paving the road for the next 3 years.

Q: What would you like to say to the GFCE community?

A: I have been involved in cyber for over 28 years, playing a role in many different areas including creating the concept of cyber diplomacy during my time in the State Department. As I reflect on my experiences, I think my new role as President of the GFCE Foundation Board presents a unique challenge and opportunity. Together with my GFCE Foundation Board colleagues, Inge Bryan and Olaf Kolkman, I am excited to help build the GFCE further, multiply its successes, and facilitate the community to achieve this. This is a great opportunity for all of us to fill a real international need; I hope people share that excitement and I hope to count on the support of the entire community to strengthen the GFCE and make a great impact together.

STAKEHOLDER ENGAGEMENT IN CYBER CAPACITY BUILDING - LESSONS LEARNED AFTER 5 YEARS OF GFCE

Written by: Daniela Schnidrig, Senior Program Lead at Global Partners Digital and GFCE Advisory Board member; and Klee Aiken, GFCE Advisory Board member

The GFCE Advisory Board is composed of civil society representatives and provides advice on the overall strategic direction of the GFCE and substantive input and recommendations. A key priority for the AB is to engage with the broader cyber capacity building community to inform the work of the GFCE. This article boils down key learnings on stakeholder engagement in cyber capacity building discussed in the AB workshop at the GFCE Annual Meeting in Addis Ababa in 2019.

There is a growing recognition that fostering a cyberspace that is free, open and secure requires multistakeholder approaches to cybersecurity policy-making and capacity building.

As a part of its role, the Advisory Board (AB) has sought to action this approach by bringing in voices from civil society, the technical community, academia, and from other perspectives

to enrich the work of the GFCE community. However, to fully realize the contributions of these communities and promote the further adoption of a multistakeholder approach, it is important to demonstrate the tangible value this model can bring. In bridging these communities within the GFCE and in capacity building activities across the globe, the Advisory Board has gained some interesting insights on how these

perspectives can enhance policymaking and capacity building that we hope to share here.

Five years after its creation, the GFCE continues to promote a multistakeholder approach to cyber capacity building, where 82 members and 27 partners, including civil society, academia and other non-governmental stakeholders, contribute to GFCE efforts regularly. The GFCE

Annual Meeting in Addis Ababa in October 2019 reflected these principles. There, the GFCE's Advisory Board hosted a workshop focused on the value of civil society engagement in cyber discussions, in particular looking at how civil society can shape cyber policy through research. Despite the workshop¹ being mainly focused on the African region, most takeaways and lessons learned are applicable in other regions as well. This article will boil down some of the key takeaways and recommendations discussed during the workshop.

Broad and Diverse Expertise

First, participants discussed the importance of understanding the breadth and diversity of the concept of “civil society” and getting beyond the stakeholder siloes that usually predominate in this field. There's a broad range of expertise in civil society - civil society actors can be policy experts, activists, academics, researchers, technologists, so reducing civil society to one label can create artificial barriers and lead us to think that civil society has a single role in cyber capacity building. This is, above all, a missed opportunity to benefit from the value that civil society actors can bring to a process.

Informed Policy is Better Policy

Civil society engagement can lead to better informed and evidence-based policy outcomes, leading to more effective implementation of the cyber policies. In its implementation, cybersecurity policy affects stakeholders



Figure 1. AB members at the GFCE Annual Meeting 2019 in Addis Ababa.

across a community. The private sector, for example, will have a unique understanding of the cyberthreats businesses face, products and services being developed to address them, and the market impact of policy proposals. Civil society organisations can bring particular expertise in the human rights implications of different policies under consideration, on the different cybersecurity threats faced by different groups within society, and experience in working directly with individuals to take steps to protect themselves online.

Bringing this expertise into any cybersecurity discussion or policymaking process can help get a more accurate and evidence-based picture of the cybersecurity landscape, the

possible implications of different policies being considered, and can build confidence and trust in the policy itself as well as with other stakeholders involved in its implementation. Stakeholders who have been involved in the development of a policy or strategy will have a stronger understanding of it and what is required from them making implementation efforts more effective.

NOTES

1

See more information in the GFCE Annual Meeting report available here:

<https://thegfce.org/gfce-annual-meeting-2019-supporting-cyber-capacity-building-for-growth/>

To be as effective as possible, cyber policies and capacity building efforts should be targeted and tailored to the specific needs of a country. The use of templates or “premade” capacity building tools was identified as a challenge by workshop participants. While they might save time at first, they are likely to miss the nuances of the cyber landscape on the ground and some key elements like trust (or lack thereof), limited resources, a country’s priorities, and the influence that the cultural context can have on the implementation of a capacity building initiative. Stakeholders input will be crucial to get a richer, more accurate picture of a country or region’s current landscape, its needs and gaps, and will help inform the design of capacity building efforts or initiatives including identifying potential challenges in implementation.

“Stakeholders input will be crucial to get a richer, more accurate picture of a country or region’s current landscape, its needs and gaps, and will help inform the design of capacity building efforts or initiatives including identifying potential challenges in implementation.”



Figure 2. AB members at the GFCE Annual Meeting 2018 in Singapore.

Sustained and holistic engagement

Stakeholder engagement cannot be done in a piecemeal fashion but should rather be approached in a holistic, sustained way. Civil society and other stakeholders need to be brought on board as partners from the get go to help craft the initiatives and provide critical input to inform the development of any capacity building effort. This will help to tailor the projects appropriately, provide a deeper understanding of the needs that the project is addressing, and it will also help increase buy-in and trust, which, as mentioned above, can contribute to a smoother implementation.

The value of research

The research that academia and other civil society actors can undertake was highlighted as a powerful tool to contribute evidence based arguments in policymaking processes and capacity building efforts, such as awareness raising campaigns.

However, a need was identified to build research into the process from very early on and to encourage a solid research base and a strong research community to make sure that research efforts respond to the needs.

“Civil society engagement can lead to better informed and evidence-based policy outcomes, leading to more effective implementation of the cyber policies.”

Finally, commitment to fund research was identified as a requisite (although not sufficient in itself) for contributing to better informed cyber discussions and capacity building efforts. It is not just about having more research but research that is more relevant



Figure 3. Participants at the workshop “Shaping cyber policy through research and capacity building” in Addis Ababa, October 2019.

to the needs and carried out in coordination with other ongoing efforts. Through the working group structures and development of a research agenda, this is a space that the GFCE can have an outsized impact.

Conclusions

Engagement across stakeholder groups and perspectives can help build more informed, sustainable, and impactful policymaking and capacity building initiatives. The growing embrace of this approach is a strong step forward that can have tangible impacts on the delivery of initiatives, however operationalizing this model still possess some key challenges. Beyond the AB workshop in Addis, AB members have had the privilege to action a multistakeholder approach in workshops and initiatives in Latin America, the Pacific, Southeast Asia, and beyond.

In working closely with policymakers, we have seen that the full value of the multistakeholder approach was not always fully realized at the outset. Creating an environment where policymakers

and other communities could engage in a direct but neutral forum, with a focus on presenting impact oriented views in policy language went a long way progressing openness to such an approach. Working together to address a common challenge is key to building that trust and the key to building better results.

Another key barrier was a lack of processes, mechanisms, and experience in bringing diverse stakeholder groups into the policy making process. The GFCE was founded in 2015 with the aim to “share knowledge and expertise, to take stock of ongoing efforts worldwide and to build international partnerships between countries, inter-governmental organisations and businesses, closely involving civil society, the technical community, think tanks and academia in the process”. The AB is one of many ways that these perspectives can be brought into the GFCE community. We hope that the lessons learned and takeaways from this article contribute to fostering a multistakeholder approach in cyber capacity building and look forward to working together to bring these views into the GFCE.

“The research that academia and other civil society actors can undertake was highlighted as a powerful tool to contribute evidence based arguments in policymaking processes and capacity building efforts, such as awareness raising campaigns.”

CAPACITY BUILDING IN THE UN CYBER-DECK: THE WINNING CARD?

Written by: Vladimir Radunovic, Director of E-diplomacy and Cybersecurity at DiploFoundation, and GFCE Advisory Board Member; and Andrijana Gavrilovic, Digital Policy Programs Assistant at DiploFoundation

Capacity building has always been among the ‘must have’ issues of cyber-related global processes and discussions. However, it was often only a buzzword, rather than an action-oriented item that should lead to establishing practical mechanisms and be supported with adequate resources. As cybersecurity has moved to the upper league of global negotiations (the UN, as well as G7 and G20, among others), capacity building has also received a more prominent role. Moreover, in the two major UN negotiations fora - the Group of Governmental Experts (GGE), and the Open-Ended Working Group (OEWG) - capacity building may end up being the strongest point of convergence. Whether a possible agreement in either will also bring substance or only the form again remains to be seen; yet there are some promising signs.

Digital challenges are increasingly positioned highly on the diplomatic agenda. As our entire economies and societies become more dependent on cyberspace, there is an increased interest in cyber security and in particular the impact of (and use of) cyberspace on international peace and security - by all states: from leading economies to the least developed countries. We can only expect it to become even more prominent, due to the sudden ‘force major’ that has pushed

us all online - the COVID-19 pandemic.

The UN under spotlight: the GGE and the OEWG

Yet, we should be aware that discussions and even deliberations about the role of ICT on international peace and security have started in the UN over two decades ago; precisely in 1998, when the first draft resolution was introduced in the UN Gen-

eral Assembly First Committee. Since then, it was mainly the GGEs - first established in 2004 by the General Assembly (A/RES/58/32), and subsequently continued in 2009/2010 (A/RES/60/45), 2012/2013 (A/RES/66/24), 2014/2015 (A/RES/68/243), 2016/2017 (A/RES/70/237), and 2019/2021 (A/RES/73/266) - that led discussions on the impact of developments in ICT on national security and military affairs.

In spite of sporadic failures to reach consensus, the GGE managed to produce a few reports of high importance, particularly in 2013 (A/68/98*) and 2015 (A/70/174), which confirmed that international law applies to cyberspace, and outlined a set of voluntary norms, confidence building measures (CBMs) and capacity building priorities. This success was certainly made easier by the fact that the GGE has had only 15-25 participants (25 in the current composition): representatives of the five permanent members of the Security Council, and a dozen of other member states, distributed based on regional diversity. In addition, discussions are held behind closed doors. The legitimacy of the consensus reports is not only strengthened by the fact that each of ‘the big five’ stood behind them, but also by the subsequent adoption of these reports by the UN General Assembly (UNGA). In addition, the current GGE is mandated to conduct a series of discussions with the regional organisation-organizations and non-participating member states, and try to feed their inputs into the deliberations. Nevertheless, this limited participation was among the arguments for looking at a more inclusive mechanism as well.

Simultaneously with renewing the GGE for the sixth time, the First Committee of the UN established the first OEWG (A/RES/73/27), based on the resolution proposed by the Russian Federation. The composition of the OEWG is open, allowing all UN member states that express a desire to participate to do so. Thus far, some 100 countries - mainly through their missions to the UN in New York and Geneva

have taken part in the OEWG meetings. In addition, the OEWG is mandated to hold informal consultations with other stakeholders. The OEWG meetings are public and streamed online.

“There was general agreement that capacity building should be demand-driven, needs and evidence-based, and non-discriminatory.”

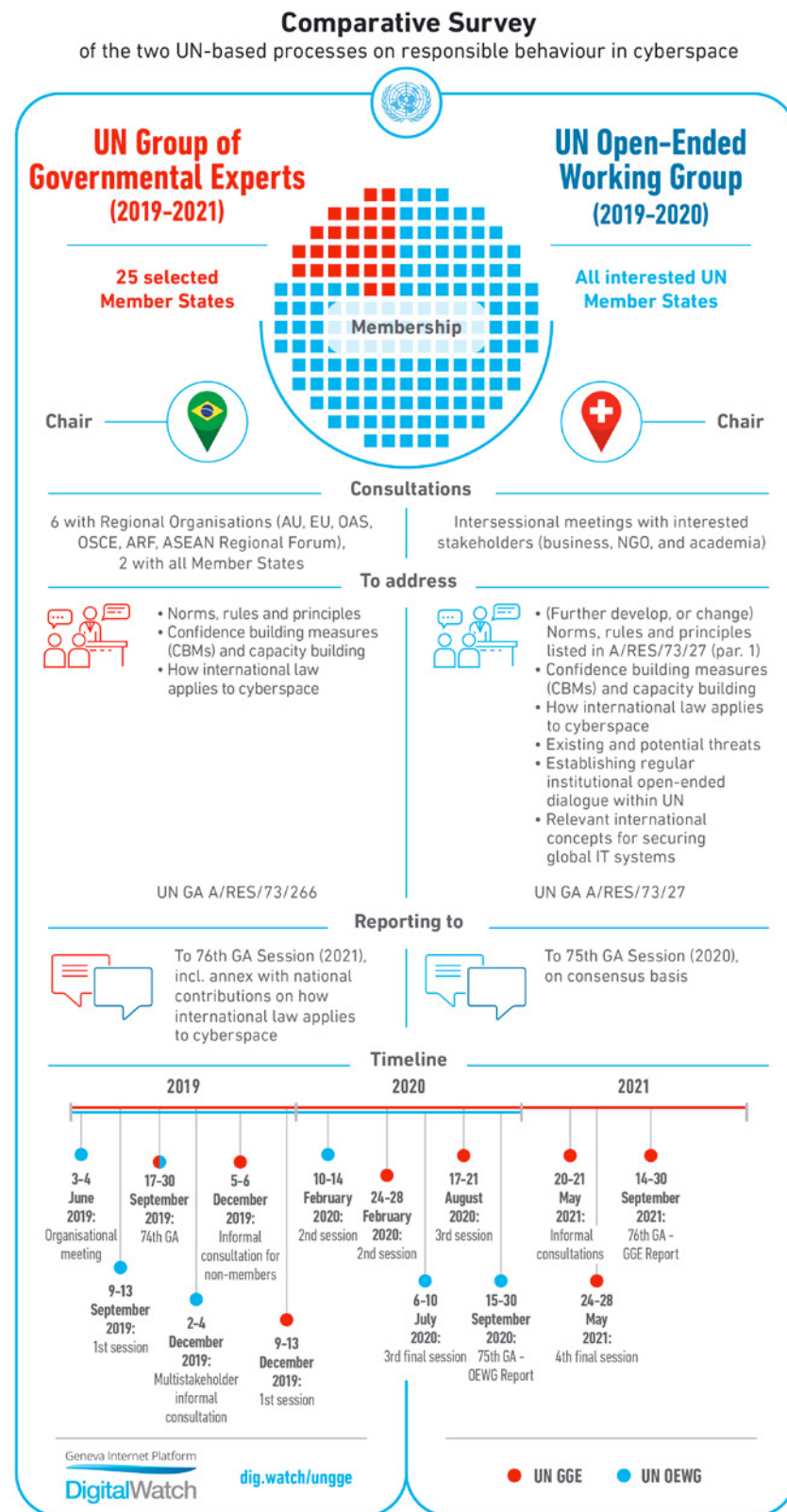
What is the difference in mandates between the OEWG and GGE then? Officially, according to the two resolutions that have established them, their mandates are pretty similar. The current GGE is mandated to study co-operative measures to address existing and potential threats in the sphere of information security (including norms, rules, and principles of responsible behavior of states), CBMs and capacity building, and how international law applies to the use of ICTs by states. The OEWG, on the other hand, is tasked to continue to develop the rules, norms, and principles of responsible behavior of states), CBMs and capacity building, and how international law applies to the use of behavior of states; discuss ways for their implementation, and to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the UN. In practice, the GGE seems to be more focused on discussing how existing international law applies to cyberspace, and possibly look-

ing into new norms. What stands out in the OEWG exchanges is related to the implementation of existing norms and CBMs, the future modality of discussions (including whether more binding rules are needed), and the capacity building measures. The OEWG should file its report to the UNGA in Autumn 2020, while the GGE has time to come up to the consensus by Autumn 2021. The infographic with the comparative survey which explains the similarities and differences in a simple manner is available, along with more details and updates on the two processes, at: www.dig.watch/ungge.

Capacity building as the possible common denominator

Capacity building is part of the mandate of both the GGE and the OEWG. Since the GGE meetings are closed to the public, it is not certain if there was any particular progress on this action item; yet it is expected that other items will dominate the agenda. In the OEWG, on the other hand, capacity building is addressed by the majority of active states. While consensus is still gloomy, some specific recommendations are emerging.

At the first substantive session of the OEWG (comprehensive reports available [here](#)), there were divergent opinions on what area of capacity building is the most urgent, and who should be in charge to move on with it - the OEWG itself, the UN, or regional organizations. A few delegations brought up the issue of funding, and several stated a multistakeholder approach to



capacity building was desirable. Informal consultations held in December 2019 (comprehensive reports available [here](#)), attended by over a hundred organizations and companies raised additional elements to be taken into consideration: capacity building needs to be sensitive to regional and national contexts; principles of national ownership, transparency, and sustainability must be respected; and capacity building activities should be coordinated to avoid duplication of efforts.

Certain convergence of positions emerged, however, at the second substantive session of the OEWG (comprehensive reports are available [here](#)). There was general agreement that capacity building should be demand-driven, needs and evidence-based, and non-discriminatory. It should also bridge digital and gender divides. The potential for synergies between capacity building, CBMs, and norms was underlined. The potential role of capacity building in achieving the sustainable development goals (SDGs) was stressed by several countries. Delegates largely agreed that existing fora should be used; the UN mechanisms, the Internet Governance Forum (IGF), as well as the Global Forum on Cyber Expertise (GFCE), were suggested in particular as potential fora for continued discussions on capacity building.

“Cyber capacity building will likely remain a common denominator in complex global diplomatic negotiations.”

The group is currently in the process of commenting on the [pre-draft report](#) of the OEWG prepared by the Secretariat. The pre-draft calls upon states to outline the principles for ICT-related capacity building efforts, and to continue to consider capacity building at the multilateral level. States are also invited to co-operate in building capacity to identify and protect national and transnational critical infrastructure, as well as the supranational critical information infrastructure. Perhaps the most interesting is the request to the UN Secretary-General to establish a global mechanism for enhancing coherence in cyber capacity building efforts, possibly in the form of a facilitation mechanism, in co-ordination with existing efforts, including on regional levels. The pre-draft report will be revised according to the first round of comments submitted by 16 April 2020. Delegates will then have the chance to comment on the revised pre-draft report. Negotiations over the draft report will take place during the OEWG’s third substantive session, currently scheduled for 6-10 July 2020.

Cyber capacity building will likely remain a common denominator in complex global diplomatic negotiations. However, whether we will see more concrete recommendations, remains to be seen - but the chances are fairly good, so far. Importantly, the existing global mechanisms for cyber capacity building - the GFCE being the lead example mentioned - will certainly have a strong role to play in either scenario.

“Importantly, the existing global mechanisms for cyber capacity building - the GFCE being the lead example mentioned - will certainly have a strong role to play in either scenario.”

Figure 1. Comparative survey of the GGE and the OEWG
(Source: [Digital Watch observatory](#))

THE AFRICAN UNION CYBERSECURITY EXPERT GROUP (AU-CSEG)

Written by: Adil Sulieman – ICT Expert, Project Manager, African Union Commission, and Secretary to the AU-CSEG

The challenge of cybersecurity facing the global community is far from being inherently technical; its economic, social and political dimensions necessitate a concerted effort for data gathering and processing to inform sound policy formulation at national, regional and continental levels. Sensing the need for rigorous and consensus-based advice on emerging issues pertaining to cybersecurity, the AU Commission (AUC) has undertaken steps to create an African Cybersecurity Expert Group (AU-CSEG), whose mandate is to advise the AU Commission on cybersecurity matters.

The need for the AU-CSEG

The African continent has made major headway in developing its digital ecosystem in the previous decade. However, there is still an evident gap among African Union (AU) Member States in terms of awareness, understanding, knowledge and capacity to deploy and adopt the proper strategies, capabilities and programs to mitigate cyber threats. The continuing digital transformation in Africa will not provide the desired social and economic benefits unless Africans have access to a secure and trusted cyberspace. Unfortunately,

rapid access to broadband in Africa in the past few years has also brought about increased cyber-criminality. While digital technologies expand the possibilities for people to enjoy freedoms and the right to access information and knowledge, reacting to emerging threats such as cyber-crime and cyber-terrorism has become a top priority of governments worldwide. The African Union Commission (AUC) sought to establish the AU-CSEG with the main objective of advising the AUC and more generally, the AU Policy Makers to pro-actively deal with cybersecurity challenges on the continent. The focus of the group will be to provide guidance and recommend strat-

egies and solutions considering the international and regional dynamics and needs. This guidance and proposed solutions aim to adopt, monitor, prevent, mitigate and address current and emerging cyber-threats and data breach and misuse.

Advice from the AU-CSEG

It has been envisaged that a core function of the AU-CSEG is to provide advice to AU on technical, policy, legal and other related cybersecurity matters at national, regional, continental and global levels. This includes but is not limited to:

1. Strategies for collecting synthesizing and disseminating information on cybersecurity for Member States;
2. Guidance on pertinent cybersecurity programs on the continent;
3. Recommend models for cybersecurity capacity building that can be adapted to meet the needs of Member State;
4. Providing guidance and advice on the online privacy and personal data protection issues raised by Member States;
5. Providing advice and support for cybersecurity sensitization programs on the continent;
6. Identifying research gaps and suggesting research areas in the field.

AU-CSEG Membership and Interests

Through a transparent selection process, ten (10) members drawn from the five African regions (northern, southern, central, eastern and western) were chosen to form the AU-CSEG, serving in a voluntary, independent and personal capacity. Two seats were reserved for each region. The Head of the Information Society division of the AUC will serve as a permanent member and a secretariat of the group.

To effectively address the multitude of cybersecurity concerns, the AU-CSEG has multi-stakeholder representation, comprised of experts from relevant Africa-wide, regional and national level organizations, institutions, academia, the technical community, civil society, and law enforcement agencies & legal institutions. Some of the group's areas of interest include:

1. Online privacy;
2. Cyber security policy;
3. ICT technology, capacity building and training;
4. Internet Governance;
5. Data protection;
6. Emerging issues, Internet of Things, Artificial Intelligence, etc.;
7. Cybercrime investigations & legislations;
8. Critical Infrastructure protection (CIP);
9. Internet and jurisdiction.

“This guidance and proposed solutions aim to adopt, monitor, prevent, mitigate and address current and emerging cyber-threats and data breach and misuse.”

Principles governing the AU-CSEG

The AU Commission strives to ensure that AU-CSEG embodies principles that will earn the group confidence and respect from AU, its Member States and African citizens. It should therefore be:

1. Open and inclusive;
2. Transparent;
3. Impartial;
4. Fair;
5. Accountable;
6. Evidence-based;
7. Consensus-based;
8. Guided by public interest;
9. Guided by the African spirit and AU Vision.



Figure 1. The AU-CSEG's first meeting at the AUC Headquarters in Addis Ababa from 10 - 12 December 2019.

In its first face-to-face meeting in December 2019, the AU-CSEG pledged towards ensuring that, among other things:

- ✓ An advocacy paper would be delivered at the AU Summit of Heads of State, held from 9 - 10 February 2020. The paper includes an overview of cyber threats in Africa, advice on emerging cyber security issues and i, International processes, and highlighted the importance of ratifying the [Malabo Convention](#).
- ✓ An action plan would be delivered aiming to support the implementation of the AU strategy that sees each African Country adopting Cybersecurity Strategy and Cyber legislation, building CERT/CIRTs and continuously building capacity at national, regional and continental levels for all stakeholders.

“As Africans, we need to articulate our own Philosophy, Ethics, Policy, Strategies and accountability frameworks for Cyberspace, Cybersecurity and Cognitive or Artificial Intelligence (AI).”

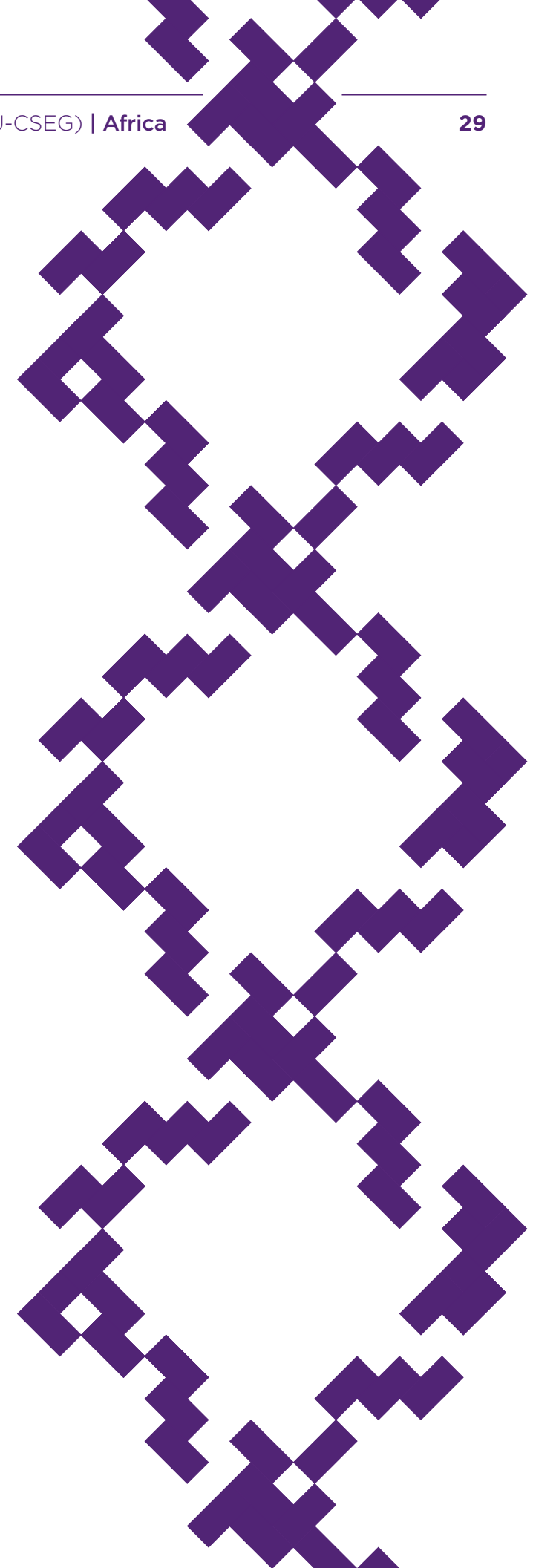
During the meeting which was held at the AUC Headquarters in Addis Ababa, Ethiopia, the group also adopted the following slogan: “As Africans, we need to articulate our own Philosophy, Ethics, Policy, Strategies and accountability frameworks for Cyberspace, Cybersecurity and Cognitive or Artificial Intelligence (AI)”.

The members of the AU-CSEG for the period of 2019-2021 are:

1. Janvier Ngoulaye (Academia)
2. Kaleem Ahmed Usmani (CERT)
3. Michael Ilishebo (Law enforcement)
4. Cecil Masiga (Policy)
5. John Ubena (Cyber legislation)
6. Houda Chihi (Academia)
7. Sherif Hashem (Academia/ Policy)
8. Abdul-Hakeem Dirisu Ajijola (Policy)
9. Nnenna Ifeanyi-Ajufo (Cyber legislation)
10. Jean-Robert Hountomey (Africa CERT)

NOTES

Special appreciation to Internet Society (ISOC) and all the independent African Experts who voluntarily assisted the AUC in this difficult selection process.



Interview

CHEIK BEDDA ON AU'S DIGITAL TRANSFORMATION STRATEGY

Written by: African Union Commission (AUC)

Mr. Cheikh Bedda was appointed Director of Infrastructure and Energy Department at the African Union Commission in October 2016, bringing to the position over 23 years' experience in the infrastructure sector. Mr. Cheikh Bedda has held several key senior positions in the Public and Private sectors and has been involved in some of the most high-profile, innovative and complex infrastructure deals in West Africa. A native of Mauritania, Mr. Bedda holds a Research Master in Sustainable Development from Université du Maine, France and a BSc (honours) in Engineering from Ecole des Ingénieurs de la flotte Maritime, Ukraine.



Figure 1. Mr. Cheik Bedda.

Q: Why is the African Union's new Digital Transformation Strategy important for Africa in 2020?

A: The Digital Transformation Strategy is important for Africa in 2020 it will strengthen the implementation framework of the African Union (AU) Digital Agenda by ensuring digitization on the Continent is done in a more coordinated manner to enhance synergies and avoid duplication of effort.

An implementation architecture and M&E framework for the Digital Trans-

formation Strategy will be developed. Development of detailed sectorial implementation plans for the Critical Sectors of the Digital Transformation Strategy (Digital Industry, Digital Trade and Financial Services, Digital Government, Digital Education, Digital Health, Digital Agriculture) will also commence.

Central to the implementation of recommendations and proposed actions detailed in the Strategy is a common thread that emphasizes the need for regional integration and harmonization of existing digitalization initiatives, projects and systems; in addition to the promotion and implementation of new initiatives.

We shall therefore kick start the implementation of proposed recommendations and actions, and its embedded linkages, to create an ecosystem of opportunities for every African and work towards the establishment of a Digital Single Market (DSM) in line with the African Continental Free Trade Area.

Q: As different African countries have differing cyber maturity, how is the priority of cybersecurity addressed by the AU?

A: Countries in Africa may have differing cyber readiness and that is the why the Strategy recognizes the diversity of contexts and situations for Members States and acknowledges the likelihood of different paces and multiple pathways towards common goals.

Previously, the AU 23rd Assembly of Heads of State and Government adopted the AU "Convention on Cyber Security and Personal Data Protection". This convention, also known as the

“A regional approach will also ensure a holistic and harmonized approach based on standards and principles, and interoperability and scalability to realize the development of a sustainable digital economy.”

Malabo Convention, seeks a common approach at a continental level on the security of cyberspace and to set up minimum standards and procedures to define a credible digital environment for developing electronic communications and guaranteeing the respect of the privacy online.

Specific to Cybersecurity, the AU Executive Council at its 32nd Ordinary Session held from 25- 26 January 2018, in Addis Ababa, Ethiopia adopted decision EX.CL/Dec.987(XXXII), which endorses the AU Declaration on Internet Governance and development of digital economy, and adopts Cyber Security as a flagship project of the AU Agenda 2063.

The convention is now open to all Member States of the African Union for signature and ratification in conformity with their respective constitutional procedures and subsequently the convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the AU of the fifteenth (15th) instrument of ratification.

“While the public sector must retain leadership, accountability and oversight capabilities for the Strategy, the role of the private sector in the implementation of the Strategy is important.”

Q: Why is a regional approach needed to drive digitalization and development of a sustainable digital economy?

A: The digital economy is fast expanding in Africa. Member States, Regional Economic Communities and the AU are adopting policies, strategies and regulations to reap the benefits of digitalization for achieving national policy goals, realizing regional and continental aspirations (as set out in the AU Agenda 2063) and meet the targets of the UN Sustainable Development Goals (SDGs).

A regional approach is needed to facilitate the establishment of harmonized policies and legal and regulatory frameworks at the regional and continental levels. This would create an enabling environment that will attract investment and foster the sustainable development of the digital economy.

A regional approach will also ensure a holistic and harmonized approach based on standards and principles, and interoperability and scalability to realize the development of a sustainable digital economy.

In summary, it would enhance continental and regional cooperation to implement the Digital Transformation Strategy for Africa, facilitate and support the establishment of regional communication networks, harmonize legislation at continental and regional levels towards a DSM and leverage synergies with existing regional and international initiatives with shared goals

Q: What are the expected challenges in implementing the Digital Transformation Strategy?

A: Challenges in implementing the Strategy include those of strengthening the coordination framework, aligning of policies and sector regulation, and the need for massive scaling-up of investment and dedication of resources.

To address these challenges, we have already initiated the process to develop an implementation architecture and M&E framework to strengthen the DTS coordination implementation mechanism. Also, the AU Commission in collaboration with other Continental Institutions and Regional Economic Communities will work with Member States to identify and address barriers to harmonization of laws and regulations and drive leadership for necessary reforms that ensure future investment in digital transformation.

We also recognize that direct linkages are necessary between public sector and private sector to realize the objectives of the Digital Transformation Strategy. While the public sector must retain leadership, accountability and

oversight capabilities for the Strategy, the role of the private sector in the implementation of the Strategy is important.

Q: How does the Strategy encourage cyber capacity building in all Member States to enable inclusive digital transformation?

A: As Member States of the AU increase access to broadband connectivity, they are becoming more interconnected and vulnerable to cyber-attacks.

It becomes critical to reinforce our human and institutional capacity to secure our cyberspace by building trust and confidence in the use of cyber technologies.

In today's digital world, personal data has also become the fuel that drives much of current online activities.

The Digital Transformation Strategy has therefore highlighted the need to support interventions to strengthen cybersecurity at the national level, to promote human and institution capacity building (public awareness campaign, professional training, R&D, Computer Emergency Response Teams, CERTs, etc.) and to build capacities of policy makers and law enforcement.

“It becomes critical to reinforce our human and institutional capacity to secure our cyberspace by building trust and confidence in the use of cyber technologies.”

Q: In the coming years, what new steps will the AUC take to ensure that all African countries are well-equipped to support the roll-out of digitalisation and handle the challenges it brings?

A: The AU Commission, in collaboration with other Continental Institutions and Regional Economic Communities, will work with Member States to identify and address barriers to harmonizing laws and regulations, and drive leadership for necessary reforms that ensure future investments in digital transformation.

BRIDGING THE GENDER GAP IN CYBERSECURITY

Written by: Organization of American States (OAS) Cybersecurity Program and Trend Micro

Today, women represent approximately 20 percent of the global cybersecurity workforce. This disparity is observed in the large gender gap in the field of cybersecurity and information, communications and technology (ICT) in general. Promoting the participation of more women in cybersecurity and ICT can bring many benefits, including the development of a more diverse workforce. Considering the increase of job opportunities in cybersecurity, securing a more diverse and prepared cyber workforce becomes essential. In order to address this gender gap, many institutions and organizations have developed initiatives to increase the role and participation of women in cybersecurity and ICT.

An uneven playing field: Women in Cybersecurity

There is currently a large gender gap in the area of Cybersecurity and Information and Communication Technologies (ICT), as there are social, institutional and personal barriers that make it difficult for more women to participate in this field. According to the [2017 Global Information Security Workforce Study: Women in Cybersecurity report](#), women represented only 11 percent of the cybersecurity workforce in 2017. This figure was even lower in Latin America, where women represented only 8 percent of the cybersecurity workforce in the region. According to Cybersecurity Ventures,

women currently account for approximately 20 percent of the global cybersecurity workforce, which is a significant increase since 2017 but still represents an extremely low figure.

The World Economic Forum foresees that 90 percent of future work will require training and skills in the area of ICT. Likewise, Cybersecurity Ventures also predicts that by 2021 there will be 3.5 million unfilled cybersecurity job openings. However, women continue to be underrepresented in this field from a very young age. As noted by the United Nations Educational, Scientific and Cultural Organization (UNESCO), less than a 3 percent of female students choose careers related to ICT. This translates into very few women transitioning into the

ICT and cybersecurity workforce. In fact, according to a report developed by the Organization for Economic Co-operation and Development (OECD), men are 4 times more likely to become ICT specialists than women are. This inequality may occur for several reasons, such as gender bias and stereotypes that are ingrained from a young age.

Considering the amount of potential cybersecurity jobs and the need for a qualified and prepared cyber workforce, it becomes essential to foster gender diversity in the field of cybersecurity and ICT, as a wider variety of cyber experts translates into a greater chance of success when solving complex cyber problems. At the same time, as more women succeed in the field of cyber-

security and ICT, they can serve as role models for other girls and women who may be interested in joining this industry.

“These efforts may require tackling gender stereotypes, raising awareness, connecting women with successful role models, and/or promoting the development of skills among girls and women.”

The participation of more women in ICT is also essential for the development of new technologies. However, currently very few women are playing an important role in this field, which can have negative impact for future technological innovation. For example, in the field of artificial intelligence, diversity has been identified as a crucial element to ensure that there is no gender bias in the development of this technology. However, according to the World Economic Forum, only 22 percent of the professionals involved in the development of artificial intelligence are women. Therefore, it is imperative to foster gender diversity in the creation of new technologies to ensure that gender bias is not perpetuated in emerging technologies, such as artificial intelligence.

Tipping the scale: efforts to increase the participation of women in cyber

Considering the existing gender gap in cybersecurity and the potential benefits that come from promoting gender diversity in this field, many governments, organizations and institutions have developed initiatives to encourage the participation of women in cybersecurity and technology. For example, the Brazilian program [Meninas Digitais](#) seeks to encourage female high school students to study subjects related to technology, by exposing them to this field and promoting the development of skills through different short courses in areas like computing.



Figure 1. Cyberwomen Challenge in Chile, June 2019.

Similarly, Mexico has developed the NIÑAS STEM PUEDEN initiative, which seeks to inspire girls to pursue career paths related to STEM, by teaching them that they are able to undertake successful careers in this field regardless of their gender. This initiative also aims at connecting and empowering young women through a Network of Mentors, in which successful women who work in STEM share their story and serve a role model for young Mexican students who are interested in this field.

As seen through the previous examples, coordinated action can help narrow the gender gap in cybersecurity and ICT. These efforts may require tackling gender stereotypes, raising awareness, connecting women with successful role models, and/or promoting the development of skills among girls and women.

“This initiative seeks to encourage the participation of more women in the field of cybersecurity and promote the development of technical skills through the organization of cyber exercises, in which only women can participate.”

OAS Cyberwomen Challenge: more women, more cyber

The Organization of American States (OAS) has a long-standing commitment to promoting gender equity in Latin America and the Caribbean, beginning with the creation of the Inter-American Commission of Women in 1928, the world's first organization of its kind. The OAS has since been at the forefront of the fight for gender equity: currently, for example, gender-related issues must be included across all its initiatives, programs and projects.

Specifically, in order to tackle the gender gap in cybersecurity, the OAS Cybersecurity Program has developed the OAS Cyberwomen Challenge with the support of Trend Micro and

funding from the Government of Canada. The Government of Canada has supported the OAS Cyberwomen Challenge since its inception in 2018. This initiative seeks to encourage the participation of more women in the field of cybersecurity and promote the development of technical skills through the organization of cyber exercises, in which only women can participate. In the setting of a controlled environment and under the guidance of an expert, the participants experience a cyberattack to a server with critical data and must solve different challenges, employing the same tools and techniques used in a real life scenario.

As a part of the OAS Cyberwomen Challenge, the OAS Cybersecurity Program and Trend Micro have organized more than 20 cyber exercises since 2018, involving over 1,000 women from 12 different countries. In 2020, the OAS Cybersecurity Program and Trend Micro hope to organize over 12 cyber exercises and involve more than 10 different countries.

SOURCES

www.ohchr.org/SP/NewsEvents/Pages/BridgingDigitalGenderDivide.aspx

www.news.un.org/es/story/2019/02/1451051

www.cybersecurityventures.com/women-in-cybersecurity/

<https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/>

www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx

www.oecd.org/internet/bridging-the-digital-gender-divide.pdf

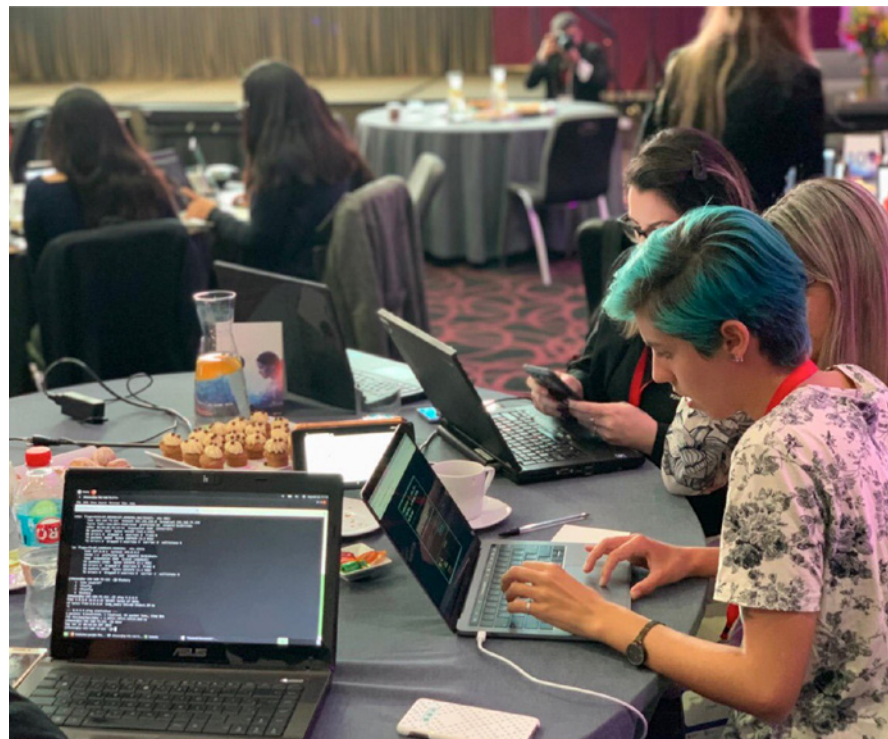
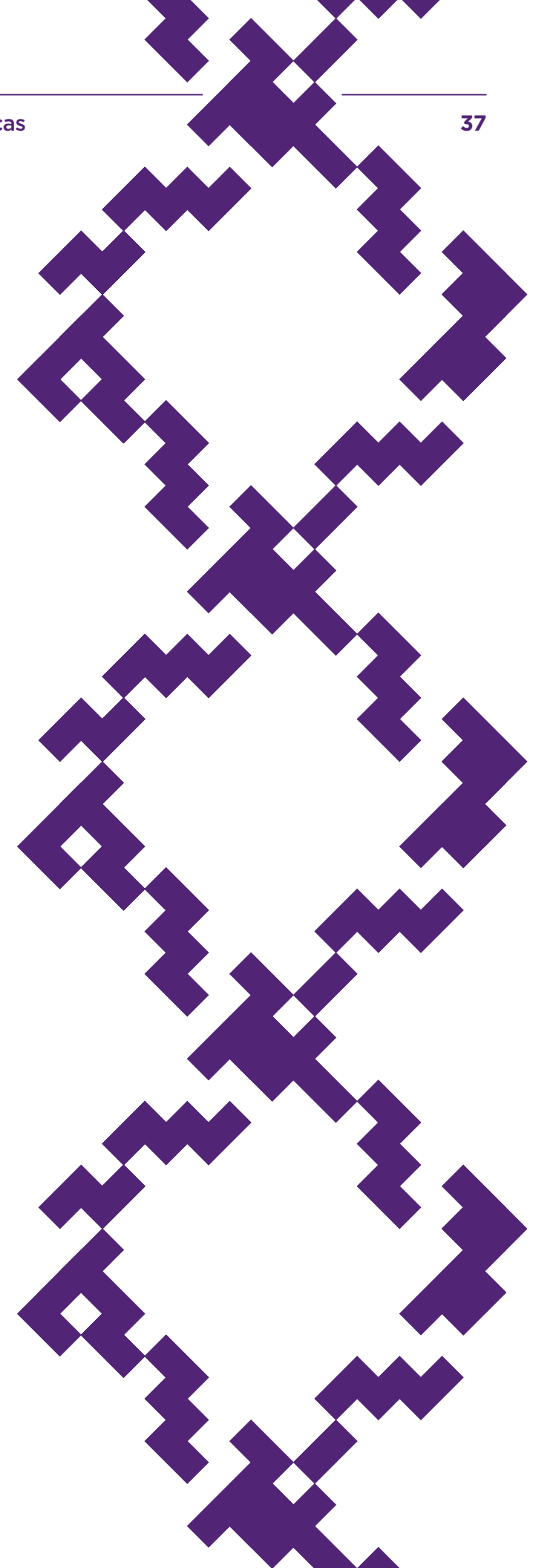


Figure 2. Regional Cyberwomen Challenge in September 2019.



Interview

STRATEGIC ROLE OF MISP ON THE REGIONAL EXCHANGE INFORMATION MODEL USED BY CSIRTAMERICAS

Written by: The Cybersecurity Program, Secretariat of the Inter-American Committee against Terrorism (CICTE), Organization of American States (OAS)

The OAS launched the first stage of the Malware Information Sharing Platform (MISP) node in 2018 through the four Pacific alliance members: Colombia, Chile, Mexico and Peru. The MISP plays a leading role in the operational framework of the hemispheric network of CSIRTs of OAS Member States (CSIRTAmericas) platform by seeking to boost a harmonized and multidirectional exchange of cybersecurity incident commitment indicators that affect Member States. This interview provides further insight on the significance of the MISP, how it is used by CSIRTs, the challenges in implementing the MISP model and more.

Q: Why is the OAS' MISP project with CSIRTAmericas important and what challenge is it trying to address?

A: The 2017 WannaCry ransomware attack demonstrated some of the major shortfalls of the global community in the sharing of cybersecurity information. The attack affected over 200,000

computers in 150 countries. This was difficult to mitigate due to the duplicity of information, the diversity of formats in shared reports, the lack of homogenization in the categorization of incidents, and above all the absence of a collaborative, knowledge-sharing mechanism. Faced with this challenge, the need to strengthen mechanisms for the exchange of actionable information arose in the Americas region.

Q: What do the CSIRTs use MISP for?

A: MISP is a free and open source project co-financed by CSIRT.lu and the European Union. The project was conceived out of the day-to-day operation of a typical CSIRT. Therefore, MISP has perfect computability with the working modalities of response teams, facilitating peer-to-peer (P2P) sharing of IOCs and cyber-threat indicators between CSIRTs.

Proof of its success is the large number of MISP multi-sector operating communities that are generated around the world. Among them, the FIRST MISP Community, NATO MISP Community, CIRCL MISP Community and all X-ISACs in different regions.

In the case of Latin America and the Caribbean, the MISP project is very attractive as it provides a collaborative, knowledge-sharing regional mechanism that is of great benefit for the countries of the region. Especially for the countries' response teams, faced with limited human resources and financial constraints.

The collective analysis and the correlation of indicators that MISP provides in the detection of attack patterns from emerging hacker groups further consolidates the work of the CSIRTAmericas community by increasing regional operational coordination and generating trust spaces between members of the CSIRTs of the OAS Member States.

Q: How is the launch of the MISP significant for your region

A: The OAS has been successful in launching the first stage of a regional MISP node through the four members of the Pacific Alliance: Colombia, Chile, Mexico and Peru. In April 2018, in Bo-

One of the main objectives of the OAS through their Hemispheric network of Computer Incident Response Teams of OAS Member States (CSIRTAmericas). This is in order to generate early alerts, prevent and minimize the response times to incidents that affect technological platforms and systems within the region.

That said, MISP enters into a leading role within the operational framework of the CSIRTAmericas platform, as a service for the region that seeks to boost a harmonized and multidirectional exchange of cybersecurity incident commitment indicators that affect our the Member States.

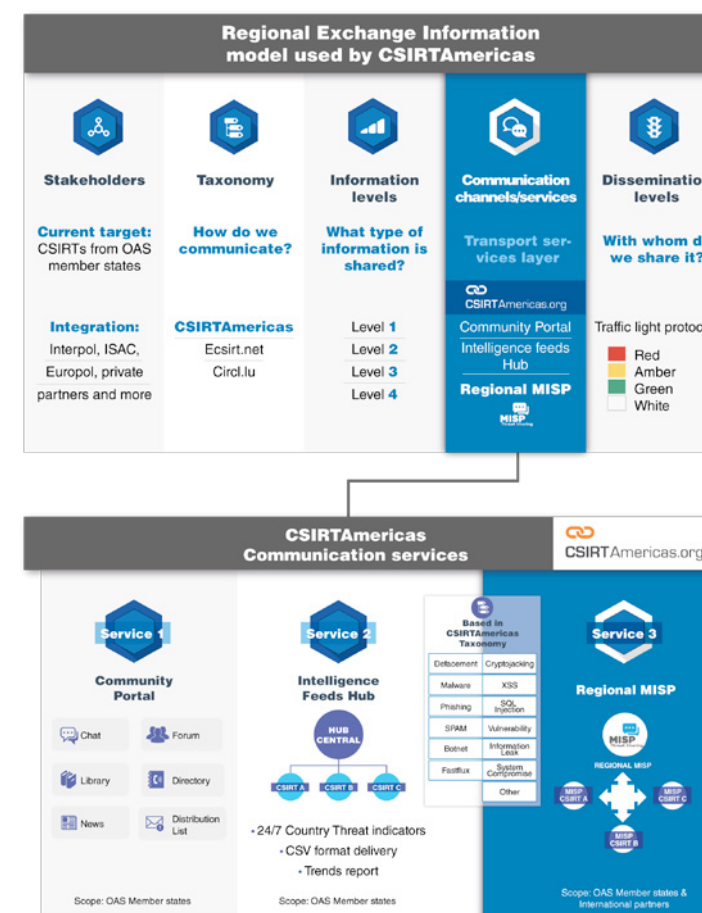


Figure 1. The Regional Exchange Information Model and its link with CSIRTAmericas Communication Services.

gota, Colombia, these four countries gathered to establish the operational guidelines in the exchange of information among their respective CSIRTs. The Inter-American Committee against Terrorism (CICTE), through its Cybersecurity Program and its CSIRT Americas Hemispheric Network (CSIRT Americas.org), was able to establish a common cybersecurity incident taxonomy to be used in CSIRT Americas network and looks to facilitate the exchange of information and notification of incidents through different communication channels (e.g. MISP) between Member States in order to contribute to the harmonization of taxonomies across the Americas region and improvement of the development of statistics on the tendencies of cyber incidents in the region.

This taxonomy allows the Pacific Alliance countries to increase the exchange of indicators of Compromise (IOCs) through MISP. Most of the cases shared have been associated with

incidents such as spear-phishing and ransomware directed at government entities, as well as BEC attacks targeting economic conglomerate companies of each respective country.

Q: What are the challenges in implementing the MISP project?

A: The main objective of the OAS is to integrate various stakeholders and improve their means of communication particularly to garner and share information. With the overarching goal of creating a sustainable model that is readily able to respond to the current and future needs of each of our Member States. Therefore, the creation and establishment of a Regional Exchange Information Model has been a permanent priority for the CICTE/Cybersecurity Program.

Some of the major challenges faced by CSIRT Americas in the implementation of MISP have been primarily two: (1) levelling technical knowledge and overall capacities, and (2) supporting an adequate level of CSIRT management. The first can be attributed to the fact that information is generally scattered, information is not centrally located making it difficult to provide guides or case-studies that are applicable to the contexts of each country and sector that seek to share information both internally and abroad. The second challenge is due to the high turnover and retention rates of the personnel within the CSIRT teams of the region. Thus, causing a lack of corporate knowledge within the CSIRTs and compromising sustainability of the overall operability of the CSIRT.

To address these challenges in facilitating sharing information in CSIRTs of the Americas region, the CSIRT Americas Hemispheric Network has focused on a model structured around five strategic pillars: (1) Stakeholders, (2) Taxonomy,

(3) Information Levels, (4) Communication Channels, and (5) Dissemination Levels. The implementation of MISP has been particularly beneficial in complementing and strengthening our fourth pillar: Communication Channels. MISP, being a model, which seeks to be flexible and harmonious, and that can be scalable to offer different services, has been useful in improving the exchange of information by allowing it to be more dynamic. This has been reflected in the share of the low-level information (“Actionable Information for Security Incident Response November 2014 – ENISA”). Easing the flow records and full packet, captures, application logs, samples of executable files, documents, and email messages between CSIRT Americas members.

Q: In what ways can the MISP project help to build cyber capacity in the region?

A: The MISP project has facilitated in levelling the capacities of our Member States in multiple ways. MISP has been integral in the creation of viable tools, the creation of flexible rules, taxonomies and formats to facilitate information sharing in different contexts and conditions. The standardization of these rules has eased the demand for the exchange of information across the region, and has incentivized greater collaboration among Member States.

Q: In what areas can the MISP be improved?

A: We have identified some areas for improvement, particularly in the presentation of case studies to design models to deploy a MISP project into a national/sectorial that requires custom contexts. This would allow a faster adoption of the tool with a multi-sectoral and broad-scale approach. We have also noticed that in the training we have

delivered, the learning curve is severely discreet, this is due to the lack of an understanding of the process map or global interaction that is applied to all of the MISP components.

Q: How has your CSIRT benefitted from the MISP?

A: In the experience of Chile's National CSIRT, the adoption of the MISP has been regarded as highly beneficial. The malwares information sharing platform has allows us to access key information to take preventive measures and thus protect our computer systems. Each of the shared commitment indicators helps reduce the security risks that are affecting other societies. The main advantage is its immediacy, which allows quick action. If one plans well, a MISP not only delivers valuable information, but also enables trust between organizations to be fostered through the platform. Its use is therefore a huge responsibility. The MISP forces [them] to have expert technicians, experienced people and bilingual professionals that can supervise or accompany its operation 24 hours a day. It is a new form of dialogue between organizations, and especially between countries. The process of coordinating the exchange links of national professionals with international ones is an interaction greatly valued and that will allows us to receive knowledge and best practices from countries that have greater capabilities. It also forces us to collaborate with those that are using our development model as a guide. The MISP project is therefore a bridge to much broader communication than the exchange of data and our vision is to promote and intensify it in that sense.



THE GFCE MEETS THE PACIFIC

Written by: Cherie Lagakali, Board Secretary, PICISOC (Pacific Island Chapter of the Internet Society); and Klee Aiken, GFCE Advisory Board member.

In February 2020, the GFCE held its inaugural regional Pacific event in Melbourne, in the margins of the OCSC-GCSCC 2020 Global Cybersecurity Capacity Building Conference. During the event, donors, project implementers and Pacific partners discussed a common goal of identifying and addressing opportunities and challenges for cyber capacity in the region. This article aims to give insight on the three core themes that emerged from these collaborative discussions: coordination, contextualization and commitment; and opportunities for further engagement with the Pacific communities.

In the third week of February, the Asia-Pacific Internet community descended on Melbourne for a number of events including [APRICOT 2020](#), [APNIC 49](#), [APTLD 77](#), the [OCSC Global Cybersecurity Capacity Building Conference](#) and a [FIRST Technical Colloquium](#).

In such a crowded field, the GFCE managed to stand out with a lively, solution-oriented Pacific Regional Forum. The event was bolstered by the gracious support of OCSC, Global Partners Digital, and the World Bank; Forum partners and members who helped with logistics and the travel costs for Pacific delegates.

For anyone working on cyber capacity building through the GFCE or in the Pacific, the room was full of familiar faces, however for most, the inaugural GFCE Pacific event was the first introduction between the different communities. With a bit of boldness in the agenda, the group was able to draw out frank insights to address a common goal of identifying and addressing opportunities and challenges for cyber capacity building in the region.

From these discussions three core themes emerged: Coordination; Contextualization, and Commitment.

While these themes are hardly unique to the Pacific, in collaboratively unpacking them in Melbourne, the group was able to gain a richer understanding of each. This resulted in a better appreciation for the different perspectives of donors, implementers, and Pacific partners, as well as, the opportunity to begin exploring pragmatic solutions to improve the way we work.

Coordination

Coordination has been at the heart of the GFCE since its inception at the 2015 Global Conference on CyberSpace



Figure 1. Pacific participants at the GFCE Pacific meeting.

(GCCS). With limited resources and a growing pool of actors, efforts to improve efficiency, avoid duplication, and amplify impact are a consistent area of focus. This need is particularly acute in the Pacific, where participants identified the challenge of limited staff resources dedicating time to attend and organize training, workshops, and consultations that were often duplicative or lacked the needed wrap around support to have a substantive impact.

In the spirit of avoiding duplication the event leveraged an existing Pacific community [mapping initiative](#) and the GFCE's own [Cybil](#) portal to build a more complete picture of activities in the region.

The community driven mapping initiative sought to draw on local expertise and knowledge and emphasized the facilitating of peer-to-peer experience sharing. Developed over the course

of independent events in Papua New Guinea and Fiji, the ongoing, crowd-sourced Pacific mapping exercise brought invaluable on-the-ground insights into the conversation in Melbourne.

“The group noted that initiatives designed with awareness of the local ecosystem, needs, and capabilities rather than driven by external KPIs or prebaked solutions were most effective.”

At the GFCE event, missing pieces of the existing puzzle were filled; particularly insights from the donor community. While far from perfect, this marriage of global perspective and local insight contributed to a more comprehensive picture of activities that can help donors coordinate funding, implementers find potential collaboration, and Pacific partners gain inspiration and learn from each other's experience directly.¹

NOTES

1

The mapping documents are available upon request; please contact Manon at the GFCE Secretariat: contact@thegfce.org.



Figure 2. Donors, project implementers and Pacific partners at the first GFCE Pacific Meeting.

In mapping these activities across the region the need for coordination came to the fore, not only between the different stakeholder groups, but also between donors themselves and implementers; as well as at the local level between government ministries and with the private sector, civil society, academia, the technical community and others.

Contextualization

While coordination offers tools for delivery, to ensure sustainable impact, the main message from the Pacific was contextualization. In experimenting with the agenda and putting Pacific voices at the center, the GFCE meeting provided a strong platform for this context to be better understood.

The group noted that initiatives designed with awareness of the local ecosystem, needs, and capabilities rather than driven by external KPIs or prebaked solutions were most effective. While predetermined solutions come with inherent shortcomings, these are amplified in a region that has its own unique challenges of scale and distance and neglect inherent advantages that local approaches and cultures provide to address common

issues. Examples shared from across the region, including the establishment of national CERTs, Internet Exchange Points (IXPs), Internet Governance Forums, and community driven initiatives such as the Samoa Information Technology Association (SITA) and Coconets – a network of women in ICT in Tonga. These examples highlighted the potential of modest initiatives with long term outlooks and flexible, grassroots approaches.

“The Melbourne event provided an important platform for on-the-ground Pacific perspectives to be shared, the development of pragmatic steps forward, and the establishment of a strong foundation to operationalize these themes.”

Commitment

While the discussion uncovered numerous opportunities for collaboration and improved approaches to capacity building, in order to action any, the group agreed that commitment was vital.

Commitment from decision makers was highlighted as important to enable initiatives at the outset and even more so for sustainability. The Pacific partners were in favor of support to raise the priority of cybersecurity on the political agenda. It was recommended that cybersecurity be sold to decision makers by stressing its contribution to sustainable development and economic growth.

Commitment to the region from donors and implementers was also seen as key to building the necessary relationships and understanding of local context for better informed projects. Additionally, this ensures efforts receive holistic support and are placed within the wider ecosystem of programs. Moving away from one-off workshops to a more strategic approach and committing to follow-up after scoping were also highlighted as key to gain traction and for

meaningful, operational goals to be achieved. This was seen as particularly important as Pacific regional approaches often received increased attention without the necessary local tailoring or follow-up to carry momentum forward

From Plans to Practice

The week began with a workshop on moving ‘From Plans to Practice.’ Although focused on incident response teams in the Pacific, the discussions there set the broader tone that resonated throughout the rest of the week. That is, the need to move beyond the rhetoric and to meaningful partnership and action. That now is time for the community to come together and to get to work.

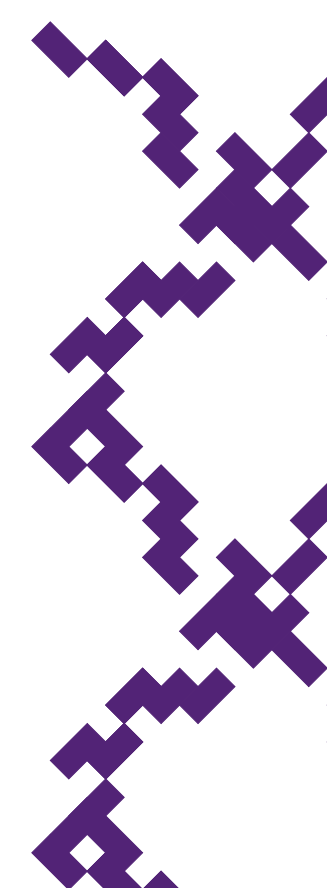
“Commitment to the region from donors and implementers was also seen as key to building the necessary relationships and understanding of local context for better informed projects.”

Although they may be different in detail or scale, the themes of coordination, contextualization, and commitment are not unique to the Pacific. Thanks to the hard work from Chris Painter, Manon van Tienhoven, Robert Collett, the GFCE, and the wider community; the Melbourne event provided an important platform for on-the-ground Pacific perspectives to be shared, the development of pragmatic steps forward, and the establishment of a strong foundation to operationalize these themes.

It was collectively agreed that the regional event and discussions were relevant, timely, and valuable for moving forward with action. Delegates welcomed more opportunities to interact directly between stakeholders, particularly between donors and Pacific partners directly.

With clear benefits to be gained by sharing Pacific experiences and approaches with the international community and adapting global good practices for the region, the GFCE working group structure was flagged as a potential avenue for real mutual value to be added. Face-to-face interactions and continuous presence were highlighted as important factors that the GFCE could facilitate, while time zone challenges led to suggestions of a Pacific friendly platform for regular regional update calls to connect across the region and exchange between the global and the local.

In these challenging times, in-person interactions will be few and far between, but with the engagement in Melbourne setting the tone, there is incredible opportunity for the GFCE and Pacific communities to work together, learn from each other, and take action. After all, who better than the Pacific share their own extensive experience for connecting remotely and what better way to leverage all the excellent cyber capacity building being done across the region.



ONLINE CAPACITY BUILDING ON CYBER LAW, CYBERCRIMES INVESTIGATION AND DIGITAL FORENSICS UNDER DIGITAL INDIA PROGRAM

Written by: N. J. P. Shilohu Rao, General Manager (Capacity Building) and Vimal Sharma, Consultant Digital India Learning Platform (LMS), National e-Governance Division, MeitY, Government of India.

With the advent of new technologies, a large section of society is reaping the benefits of the cyber world using mobile phones and IT systems. This has simultaneously led to a phenomenal increase in cybercrimes that pose a major challenge to the Law Enforcement Agencies in dealing with them. Threats from cyber criminals are going to be even more pronounced in the coming years, with the emergence of 5G Ecosystems, digital economy, the Internet of Things (IoT), amongst others. This has resulted in the immense need for a large proportion of the trained police force, prosecutors and judges to be equipped with necessary skills to maintain law and order. This article is about imparting an online Capacity Building Program on Cyber Crimes and Laws using the Digital India Learning Platform (LMS) to law enforcement, judicial officials, etc. In a global context, online capacity building will help governments to exchange knowledge faster and with ease.

Prosecuting Cybercrimes

Unlike crimes in the physical world, the crimes in the cyber world are quite different. The electronic evidence needs to be preserved and protected for the purpose of the prosecution of

crimes conducted in cyberspace. As electronic evidence cannot be physically seen, it must be capable of being analyzed using special tools. Studying, analyzing and understanding cybercrimes requires the use of tools or knowledge of forensics and the process must be documented, reliable and repeatable.

Most importantly, the nature and extent of cybercrimes and the electronic evidence should be understandable to the prosecutors and the courts to punish the culprits. A planned and holistic training is necessary to close the gap of techno legal skills required by those handling cybercrimes. Furthermore, every Law Enforce-

ment Agency (LEA) is expected to have the techno-skilled manpower in digital forensics and possess the licensed tools to demonstrate the reasonable competence for court trials.

Cybercrimes have been increasing with an alarming rate throughout the world, making it even more of a challenge for LEA and Judiciaries to resolve cases properly with time. To overcome the challenges in the process of investigations and disposal of cases, it is imperative to build capacity of the stakeholders in a way that learning becomes easy and effective by complementing their daily, ongoing job.

“The program aims to bring experts from law universities and institutions, police academies and industries to build the capacity of officials with skills of cyber laws and digital forensics.”

The challenges faced

From the data published by India's National Crime Records Bureau (NCRB), it is evident that LEA and Judiciaries are facing challenges in recent years as cases pendency is increasing at a high rate while case disposals rate is much lower in comparison. Some of the common challenges which are prevalent among the LEA and Judiciaries are:

1. Most LEA are facing problems with the growing menace of social media. The crimes are committed in the form of defamatory articles, fake news, trolling and mischief to create unrest or disturbances in law and order.
2. In some cases, the internet intermediaries do not respond with the required information in a timely manner, which is required to prevent the cybercrimes. The intermediaries insist that they go through the MLAT even for seeking basic information for prosecution purposes. Despite the MLAT not being required in several cases, due to lack of knowledge in cybercrimes and laws, the Agency is compelled to adopt MLAT routes which is a time-consuming exercise.
3. Acute shortage of trained manpower is the major stumbling block for LEA. Due to the lack of trained (technical and skilled) manpower in the state and central LEA, effective prosecution pertaining to cybercrimes is always in limbo.
4. Even where a prosecution is successful, the ability of judges to appreciate the evidence

and decide on the ruling of cases involving ever-changing technologies is another equally important concern.

India's Online Capacity Building Program

With the above challenges in mind, the National e-Governance Division (NeGD), under the flagship program 'Digital India' formed by India's Ministry of Electronics and IT (MeitY), has initiated an Online Capacity Building Program on Cyber Law, Cybercrime Investigation and Digital Forensics through its learning management system (LMS).

The objective of the program is to equip Police Officers, LEA, Prosecutors and Judicial Officers with the necessary skills to deal with cybercrime cases using digital forensics in an efficient and effective manner in accordance with India's laws, and adopting best practices, standards and guidelines from across the world.

The program aims to bring experts from law universities and institutions, police academies and industries to build the capacity of officials with skills of cyber laws and digital forensics. Under the program, NeGD will offer 'Online PG Diploma in Cyber Law, Crime Investigation & Digital Forensics' in a phased manner to 1000 officials including Police, LEA, Prosecutors and Judicial Officers through the LMS. This program will be conducted nationwide through a 'hub and spoke' model and in collaboration with consortium partners: NLIU (Bhopal) and other law universities like National Law University (Delhi), National Law School of India University

Salient Features of the E-learning System

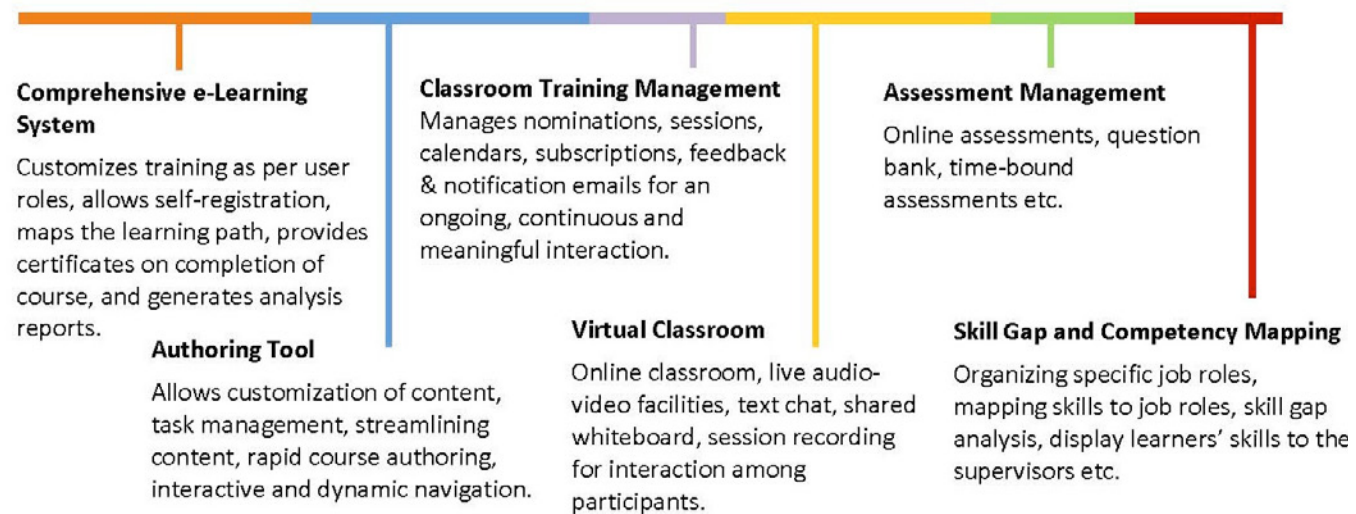


Figure 1. The salient features of the Learning Management System used for the Online Capacity Building Program.

(Bangalore), Rajiv Gandhi National University of Law (Patiala), etc. The diploma will be delivered through blended learning as follows:

- 70% of the course will be delivered using LMS;
- 20 % will be conducted through lab sessions and simulation of case studies and scenario-based learning;
- 10 % will be project work on job-based projects;
- Additional post-certification workshops in the form of webinars.

“With new technological advancements and innovations arising every six months, the lifecycle of technological products and services are short, highlighting a need for LEA and Judicial to stay aware and updated in order to combat cybercrime effectively.”

Advantages of an online Program

This online program facilitates continuous, systematic learning for the learners in a blended training format. It enables learners to experience anytime anywhere learning on the go, without displacing them physically. This program will include e-content and live online sessions in the form of webinars from various industry experts & academia. In addition, each enrolled trainee will undergo instructor-led practical classroom training at the designated cyber forensic lab for a period of two weeks. As a result of the program, the expected outcomes are:

- PG Diploma in Cyber Law, Cybercrime Investigation and Digital Forensics will be awarded to 1000 participants on completion of this course;

- A state-of-the-art Cyber Forensics Lab for continuous training in public private partnership mode with involvement of academia and private partners;
- 100 hours of world class e-Content in the form of webinars and e-learning modules for training purposes;
- Increase in number of skilled resources within the targeted groups of State Police, LEA and Judiciary.

It is envisaged that the Online PG Diploma will be a milestone in building a robust and sustainable Capacity Building System. Wherein Governments, Law Experts and Technology Experts will be associating and partnering to combat the expo-

ponential rate of cybercrimes across the world. The importance of imparting time-bound training is needed to ensure the program's relevance to the current context of cybercrimes. With new technological advancements and innovations arising every six months, the lifecycle of technological products and services are short, highlighting a need for LEA and Judicial to stay aware and updated in order to combat cybercrime effectively. The Online Capacity Building model described in this article serves various purposes such as promoting the self-learning culture, providing a single platform for diverse learning needs and providing the latest and most relevant information with regards to the skills required by the LEA across the world.

“Studying, analyzing and understanding cybercrimes requires the use of tools or knowledge of forensics and the process must be documented, reliable and repeatable.”

ADVANCE LEARNING	
Accessibility ■	Seamless Trainings ■
Anytime	Online training delivery
Anywhere	Virtual Classes/Webinars
Online	Flexible blended training
	Business Intelligence & Analytics ■
	Reports generation
	Managing learning requirements
	Feedback Analysis
	Progress of Trainees
	Flexibility ■
	Self paced training
	Training delivery
	Organizing training
	Continuous learning
	Evolved Content ■
	Updated Content / Courses
	Aligned to global standards

Figure 2. Advantages of online advance learning through the Online Capacity Building Program.

Interview

MIGUEL GONZÁLEZ-SANCHO ON EUROPE'S DIGITAL SINGLE MARKET AND CYBERSECURITY

Mr. Miguel González-Sancho was appointed Head of the Unit "Cybersecurity Technology and Capacity Building" at the European Commission in July 2018. Miguel has worked at the Commission for over 20 years, mainly on EU policy and 'R&D&I' programs relating to digital technologies, and previously on telecoms regulation and trade policy. His previous responsibilities in the Commission include Head of Unit for eHealth, Head of Unit for Administration and Finance, Deputy Head of Unit for Policy Coordination, Deputy Head of the Unit for eInclusion, and member of cabinet of a European Commission Vice-President. Miguel holds degrees in law, international relations, business administration, accounting and auditing.



Figure 1. Mr. Miguel González-Sancho

Q: What is the digital single market and why is cybersecurity important?

A: Basically, the digital single market is about EU citizens and business acquiring and providing goods and services online, while benefiting from equivalent rights and safeguards that is provided in the physical single market. This is only possible if digital transactions have an appropriate level of security, which in turn will determine the level of trust from citizens and business.

Q: How is your unit involved in making progress towards a European digital single market?

A: Unit CNECT.H1 "Cybersecurity Technology and Capacity Building" is a policy unit, i.e. we do not provide operational cybersecurity services but support others doing so in two main ways: cooperation and building capacity.

First, we support cooperation amongst EU cybersecurity players, notably national authorities. For instance, in cooperating to coordinate their response to major cyber-attacks, or to agree on a common approach to identify the cybersecurity risks associated with 5G networks and the measures to mitigate those risks.

Second, we mobilize EU programmes to financially support cybersecurity research and implement cybersecurity solutions in the EU. In doing so, we work not only with national authorities but also with businesses and academia.

Q: What is the most important thing to consider when addressing new security risks relating to new ICTs (e.g. 5G)?

A: Typically, the three key elements to consider in cybersecurity are technology, people and processes; all three must be addressed by those responsible for delivering cybersecurity, by public authorities or businesses. From our EU cybersecurity policy perspective, we aim to develop a framework where all Member States ensure a certain level of cybersecurity commitment and preparedness, ongoing exchange about their national approaches and experiences, and agreement on some common prior-

ities (such as in the case of 5G cybersecurity mentioned in the question), which can be supported with EU funding.

“The most important aspect to consider when addressing new security risks: purely individual or national solutions are not enough.”

The involvement of Member States is essential because cybersecurity is very much their legal prerogative, rather than an EU prerogative. At the same time, there is an important internal market dimension to cybersecurity, insofar as it is an essential enabler of the digital single market which transcends national borders, just like how cyber threats knows no borders either. That is perhaps the most important aspect to consider when addressing new security risks: purely individual or national solutions are not enough. It is therefore key to share at various levels: goals, capacity, information, etc.

Q: Why is capacity building important for cyber resilience and what capacity is needed to respond to such cyber threats?

A: Cyber resilience is a very practical matter, beyond awareness which is very important, it requires dedication and resources, to an extent that varies according to the assets to be protected and the level of exposure. It requires human and technical capacity to face cyber threats that are constantly evolving, so the response must also evolve accordingly.

Q: What practical steps does your unit take to ensure that there is the necessary capacity to respond to such threats?

A: Something very practical we do is manage parts of the EU programmes supporting cybersecurity research and deployment through European public funding. For this, we regularly:

1. Define the funding priorities while considering the relevant feedback from cybersecurity stakeholders;
2. Organise the calls for proposals and their selection;
3. Monitor that the selected consortia deliver, according to their contractual obligations (i.e. that EU funding is effectively contributing towards the cybersecurity priorities initially defined).

This can range from a research project on artificial intelligence for cyber resilience, to a platform for cooperation between EU computer security incident response teams (CSIRTs). Most projects involve a number of EU organisations, which reflects in practice the importance of cooperation in building capacity for cyber resilience.

Q: What are the challenges that your unit faces and how do you overcome these challenges?

A: As much as the future of our society and economy must be sustainable in terms of efficient use of natural resources, it will also be digital. Sustainable digital development requires sufficient cybersecurity, otherwise, our digital dependence can seriously compromise our citizens, businesses and

ultimately, our way of life. In that regard, one big challenge for the Commission, and the EU as a whole, is to step up our game on cybersecurity cooperation and capacity. This requires Member States to agree to more ambitious common EU priorities on cybersecurity. For this, the Commission has proposed to review the Directive on Security of Networks and Information Systems ("NIS Directive") this year, which is the first and main EU legislative instrument on cybersecurity.

Secondly, it means that the common EU priorities shared by all Member States are implemented, notably by pooling investments in strategic areas where the EU wants to build strong cybersecurity capacity, thus contributing to its technological sovereignty. Therefore, the Commission has proposed a Regulation on a European cybersecurity centre and network of national centres, which will decide and implement cybersecurity investment priorities in Europe. Our immediate challenge in that regard is that the Council of the EU and the European Parliament adopt that Regulation, and then the Commission together with Member States and other relevant actors identify what are the priority areas to be supported.

All of this is certainly challenging, considering that the cybersecurity landscape across the EU is rather fragmented, in terms of legal competences, market players, etc.

Q: As the head of the unit, can you share lessons learnt in building cyber capacity for the digital single market?

A: One important lesson for me is that when designing and implementing EU cooperation efforts on cybersecurity across Member States, it is essential for the Commission to work alongside those responsible for cybersecurity in the Member States. That is the main asset

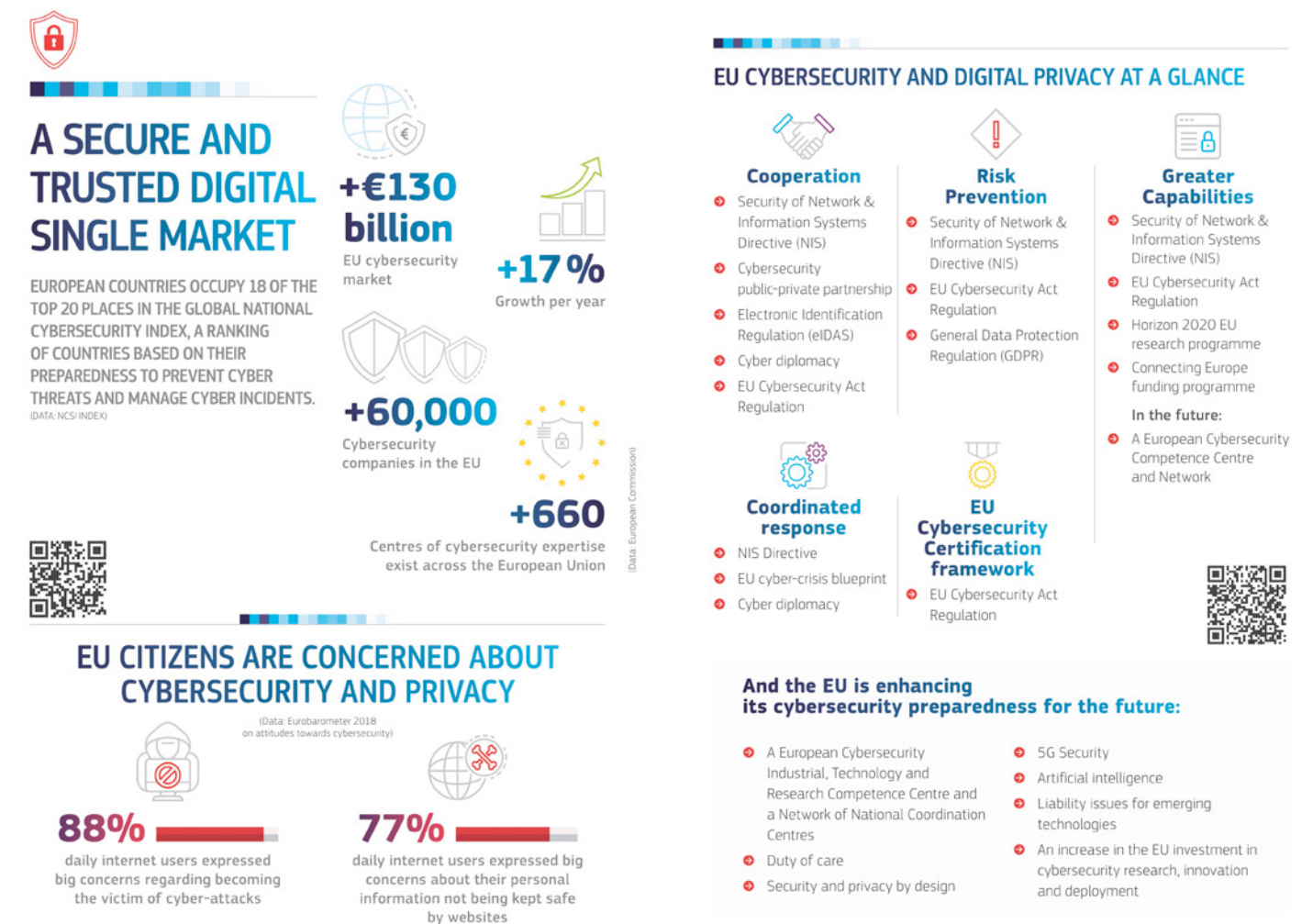


Figure 2. An Infographic on the Digital Single Market and EU Cybersecurity and Privacy.

of the Cooperation Group of the NIS Directive, integrated by representatives of all EU Member States, the Commission and the European cybersecurity agency – ENISA. The NIS Cooperation Group has delivered many successful examples of such EU cooperation driven by consensus, including those already mentioned on coordinated response to major cyber-attacks or cybersecurity of 5G.

Something comparable applies to EU industry, with whom the Commission has been remarkably collaborating with on our Contractual Public Private Partnership on cybersecurity. I feel a growing momentum in that regard; a

shared realisation by all relevant EU actors that to address raising common cyber threats and therefore ensure sustainable digital development, cybersecurity cooperation and capacity must be significantly increased in the EU. The challenge is how the EU will manage to do that, and how fast.

EU CYBERNET - THE NEW KID ON THE EU CYBER CAPACITY BUILDING BLOCK

Written by: Siim Alatalu, Estonia Head of EU CyberNet

It has now been 7 years since the EU adopted its first strategy for dealing with cyberspace. The 2013 “EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace” inter alia urged the European Commission to recognize the need to develop cybersecurity capacity building initiatives. By now, the EU as well as other players have launched several cyber capacity building projects and a lot of good work on building partner countries’ cyber capacity is done around the world. Yet, as no country can be ‘cyber ready’, a new initiative funded by European Commission’s DG DEVCO was launched in September 2019 – the EU CyberNet. This article will explore what makes this new project unique and how it could support and complement the EU’s ongoing efforts in cyber capacity building.

European Cybersecurity and Capacity Building

The past dozen years have seen an unprecedented increase in the global connectivity offered by the Internet, providing for real-time interaction in all areas and in almost all societies, thus encouraging countries to pay more attention to enhancing their national cyber security capacity. Despite already celebrating its 50th anniversary last year, the Internet serves the global community with increasing vigor – and thereby increasing the need for building global cyber capacity.

At the time of writing this article, end of January 2020, we have another important anniversary. It has now been 7 years since the EU adopted its first strategy for dealing with cyberspace. One of the outcomes of the January 2013 “EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace” is that it urged the European Commission to recognize the need to develop cybersecurity capacity building initiatives. At that time, their focus was on police and judicial cooperation in third countries and to advance coordination of relevant stakeholders in order to avoid the duplication of efforts.

What we can observe now is that it also launched a series of developments in the cyber security of the EU as well as the development cooperation communities.

Combining the two perspectives, the 2013 EU Cybersecurity Strategy was followed by the adoption of the European Agenda on Security in 2015 and the New European Consensus on Development in the spring of 2017. In the fall of 2017, during the Estonian EU Presidency, the Council of the EU took the strategy forward in its Conclusions on the Joint Communication “Resilience, Deterrence and Defense: Building

strong cybersecurity for the EU” where it called for the EU and its Member States to promote cyber capacity building in third countries by setting up an EU Cyber Capacity Building Network. To close this circle of conceptual developments and after 5 years of conceiving the original idea, the Council concluded an agreement on the “EU External Cyber Capacity Building Guidelines” in 2018. The time was ripe for the joint practical implementation of these interlinking ideas and strategies.

The EU CyberNet

The EU Cyber Capacity Building Network, or EU CyberNet (or project number IFS/2019/405-538) started in September 2019, for a planned duration of four years. Fortunately, after six years since the idea was first described in the EU Cybersecurity Strategy, it did not enter an empty playground. Over the course of time, both the EU and the other players such as notably the GFCE, had already launched several capacity building projects. To name a few prominent ones such as GLACY, GLACY+, CyberSouth and Cyber4Development, they focus specifically on developing areas such as cybersecurity policies, institutional setups, fight against cybercrime, and public diplomacy in countries outside of the EU. Many countries and hundreds of people around the world have already benefitted from the good work by these projects by way of education, training and networking. A pragmatic reader may thus ask the question, what makes EU CyberNet unique or special amongst them? What is its particular benefit?

“The strategic cyber challenge for both the EU as well as the individual Member States is that with the constant development of technology and the need for new skills, no individual, country or organization can ever be ‘cyber ready’.”

The strategic cyber challenge for both the EU as well as the individual Member States

is that with the constant development of technology and the need for new skills, no individual, country or organization can ever be ‘cyber ready’. While more than half of the world’s population is online, this ‘race’ against moving targets will forever be hard to win. There are, however, clear rewards on sight for at the minimum trying to stay in the game – for instance, the World Bank estimates that a 10% increase in access to the internet leads to a 1.3% increase in GDP. Ensuring the safety of cyberspace for embracing the internet should therefore be seen by states as one of the preconditions for increasing welfare of their citizens and societies. This in turn requires investment into both technical capabilities as well as people and their capacity in cyber security.

The linkage between individual’s cyber security skills and the cyber security of a nation is undeniable. According to fact-sheets by the EU Cyber Direct, in the last five years there has been



Figure 1. An EU CyberNet presentation slide outlining the shared challenges in building cyber capacity.



Figure 2. EU CyberNet on display at the EU's cyber booth during FIC2020 in Lille, France.

a 67% increase in cyber security breaches. Cyber-attacks do not favor or discriminate targets as was evident in particular in 2017, when two global malware attacks WannaCry and NotPetya infected over 300,000 computers, spread to more than 150 countries and caused more than \$4bn in economic damage (and due to the legal spill overs, the final financial count is still not clear). Regardless of how uncomfortable bringing the bad news feels, the problem will only grow and is expected to be particularly

far-reaching in the 2020s as the world moves from fourth-generation information networks to the fifth, introducing a significantly higher technological capacity.

Better Coordination and Cooperation

The purpose of EU CyberNet is twofold. On one hand, it will strengthen the global delivery, coordination and coherence of the EU's external cyber capacity building projects. In other words,

complement and enhance all the good work that is already ongoing. On the other hand, EU CyberNet will reinforce EU's capacity to provide technical assistance to third countries in the areas of cybersecurity and countering cybercrime. In other words, it seeks to bring together the comprehensive cyber security competence available in the different EU Member States to participate in the EU's external cyber capacity building efforts. Given the borderless nature of cyberspace, it should be clear that the cyber security of the EU begins outside its borders. The bottom line is: the better the cyber security capacity of likeminded countries abroad and the better the direct contacts between the European cyber defenders with their peers, the better the cyber security will be in EU Member States.

EU CyberNet has set to deliver four objectives that are:

1. Establishing a network of experts and stakeholders. The quantitative ambition is to establish 'Cyber Team EU' that has at least 500 individuals from the different cyber security domains (from technology to strategy, from counter-cybercrime to international law) as well as at least 150 institutions (from the national cyber authorities to academia and think tanks) sign up to the EU database as a stakeholder community.
2. A Training and Assistance Capability that entails a library of courses and/or training modules that are available to partners from outside the Union and implemented by experts from the EU database.



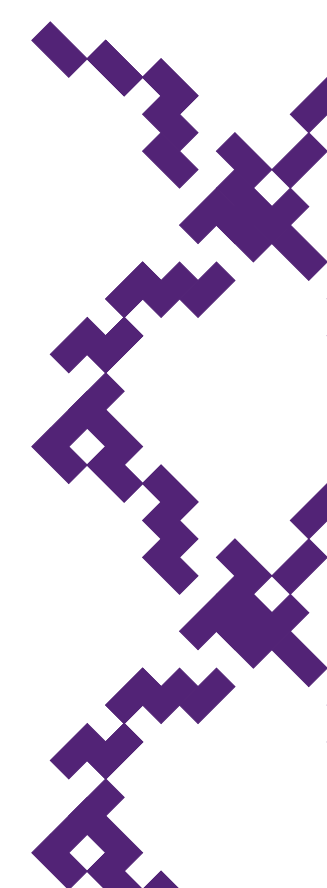
Figure 3. EU CyberNet's first training event for the European Commission's cyber projects in March 2020.

3. Central Processing for EU's External Cyber Engagement – the EU CyberNet is to evolve into a coordination platform for the various cyber security initiatives that the EU is already implementing and provide up-to-date information for example for the European Commission services.
4. The technical Online Platform is to become the online home and front-end of the project, featuring the capability for example information exchange relevant to the stakeholders, donors and beneficiaries.

EU CyberNet is a joint project of the European Commission DG DEVCO and EU Member States. Implementing the EU CyberNet builds on the cyber security strengths of the lead contractor, Estonian Information System Authority RIA and its consortium partners in Luxembourg, Germany and Finland. However, the ambition as outlined above is to reach out to all the competent authorities in the EU and cyber experts in different fields who share the

understanding of how important cyber security is and will be for both their nations as well as for the entire European Union. In this vein, we look forward to cooperation with likeminded partners. This is a shared playground and by working together we can perhaps even win this game.

“Given the borderless nature of cyberspace, it should be clear that the cyber security of the EU begins outside its borders.”





Meet Cybil.

The globally owned one-stop knowledge hub that brings together knowledge on international cyber capacity building.

570
projects

A repository of past and present international cyber capacity building projects.

72
tools

Resources to help design and deliver international cyber capacity building projects.

73
publications

Lessons learnt, outcomes and research about international cyber capacity building.

421
actors

Governments, companies and organisations involved in international cyber capacity building.

39
events

Overview of upcoming regional and global events related to cyber capacity building.



PORTAL GROUP



DIPLO



Global Cyber Security Capacity Centre



Norwegian Institute of International Affairs

www.cybilportal.org

Got an initiative, report, event to share? Get in touch with us via the portal.

Volume 7, April 2020
**Global Cyber
Expertise Magazine**

Colophon

Editorial Board:

Moctar Yedaly (AU)
Carlos Bandin Bujan (EU)
Belisario Contreras (OAS)
Kathleen Bei (GFCE)

Guest Editors:

Daniela Schnidrig
Klee Aiken
Vladimir Radunovic
Andrijana Gavrilovic
Chris Painter
Cherie Lagakali
N J P Shilohu Rao
Vimal Sharma
Cheikh Bedda
Adil Sulieman
Siim Alatalu
Miguel Gonzalez-Sancho
Chile's National CSIRT
Trend Micro

Artwork & Design:

Roguer Restrepo Estrada (Colorful Penguins)

Chief editor:

Kathleen Bei (GFCE)

Publishers

African Union, www.au.int, contact@africa-union.org,
@_AfricanUnion

European Union, www.europa.eu, SECPOL-3@eeas.europa.eu, @EU_Commission

Global Forum on Cyber Expertise, www.thegfce.org,
contact@thegfce.org, @theGFCE

Organization of American States, www.oas.org/cyber,
cybersecurity@oas.org, @OEA_Cyber

Disclaimer

The opinions expressed in this publication are solely those of the authors and do not necessarily reflect the views of the AU, EU, GFCE or OAS, or the countries they comprise of.

Global Cyber Expertise Magazine

**AU • EU • GFCE • OAS
contact@thegfce.org**

**Issue 8 submission deadline:
14 August 2020**